

Exploring the Implementation of Data Protection in A Private Institution: Basis for A Strategic Action Plan

Jeriko Arwel S. Arlegui

Graduate Studies Student, National University, Sampaloc Manila, 1008 Metro Manila, Philippines

Publication history: Received: May 19, 2026; Revised: June 4, 2026; Accepted: June 9, 2026

Email of Author: jasarlegui@nu-fairview.edu.ph

Abstract

This study examined the implementation of data protection among Senior High School faculty at NU Fairview and developed a Data Protection Strategic Action Plan to strengthen institutional compliance and information security. Anchored on Protection Motivation Theory (PMT), the study explored faculty perceptions of data threats, efficacy in safeguarding student information, existing data protection practices, and barriers affecting compliance. A convergent parallel mixed-methods design was employed, integrating quantitative and qualitative data collected from 45 full-time faculty members through a researcher-made Protection Motivation Appraisal Survey and a semi-structured interview guide. Forty-four faculty members completed the survey, while eight representatives participated in a Focus Group Discussion. Quantitative data were analyzed using descriptive statistics, while qualitative data underwent deductive thematic analysis, followed by data integration through a Joint Display Method. The findings revealed that faculty members demonstrated high awareness of data protection risks and consistently practiced physical and digital safeguards, including data minimization, access control, secure communication, and responsible document handling. However, compliance efforts were constrained by infrastructure limitations, inadequate cloud and physical storage facilities, operational burdens, knowledge gaps, and insufficient policy dissemination. Faculty reported confidence in routine data protection practices but showed lower confidence in technical competencies and formal reporting procedures. The convergence of quantitative and qualitative findings further revealed that many compliance behaviors relied on self-developed workarounds rather than structured institutional support. The study concluded that while faculty possess strong protection motivation, institutional barriers hinder consistent and sustainable compliance. Consequently, the study recommends implementing a Data Protection Strategic Action Plan focused on infrastructure enhancement, policy operationalization, targeted training, and reduced operational friction. This study supports SDG 4 (Quality Education), SDG 9 (Industry, Innovation and Infrastructure), and SDG 16 (Peace, Justice and Strong Institutions) by promoting secure educational environments, responsible digital governance, and strengthened institutional accountability. Its sustainability contribution lies in enhancing educational, technological, and institutional sustainability through improved data governance, privacy protection, and information security practices.

Keywords: Data Protection Strategic Action Plan, Data Protection Practices, Educational Data Privacy, Information Security, Protection Motivation Theory, Senior High School Faculty

1. Introduction

The increasing digitalization of education has transformed the management of personal information, making data protection a critical institutional responsibility. Educational institutions collect and process large volumes of sensitive student data through digital and physical systems, requiring compliance with legal, ethical, and technical standards. Despite existing regulatory frameworks, challenges in implementation persist due to human, organizational, and technological factors. This study explores the implementation of data protection among Senior High School faculty at NU Fairview and develops a Data Protection Strategic Action Plan to strengthen institutional compliance and security.

1.1 Background of Data Protection Implementation among SHS Faculty

The global expansion of digital education has elevated data protection as a fundamental component of institutional governance and trust (UNESCO, 2024). International frameworks such as the Modernized Convention 108+ (2018), General Data Protection Regulation (GDPR), ASEAN Model Contractual Clauses (2021), and ISO/IEC privacy standards emphasize the protection of personal information and ethical data processing (Council of Europe, 2021; ASEAN, 2021; ISO/IEC, 2023). While educational technologies support innovation and personalized learning, they also increase risks related to unauthorized access, misuse, and disclosure of personal information (Tzimas & Demetriadis, 2021; Kaye et al., 2024; Vlieghe et al., 2023). In the Philippines, Republic Act No. 10173 or the Data Privacy Act of 2012 mandates the protection of personal and sensitive information, including educational records. Educational institutions are required to uphold transparency, proportionality, and accountability through mechanisms such as Data Protection Officers and Privacy Impact Assessments (DPA, 2012). However, incidents such as the 2024 Department of Education data leak and

unauthorized access to university records in 2025 demonstrate continuing vulnerabilities (NPC, 2024). At NU Fairview, institutional efforts to strengthen privacy compliance have been established through the appointment of compliance officers and local privacy oversight mechanisms (Calub, 2026). Nevertheless, reported incidents involving unauthorized disclosure of student information suggest gaps between policy and practice, highlighting the continuing influence of the human factor in data protection implementation (Sangwan, 2024; MDPI, 2026). These conditions necessitate the development of a localized Data Protection Strategic Action Plan.

1.2 Themes and Insights from Related Literature on Educational Data Protection

Protection Motivation Theory (PMT) explains protective behavior through threat appraisal and coping appraisal processes (Rogers, 1975, as cited in Rogers, 1983). Individuals are more likely to engage in protective actions when they perceive threats as severe and probable, believe that protective measures are effective, possess confidence in their abilities, and perceive lower response costs (Rogers, 1983; Designing a Digital Health Intervention Using PMT, 2025). PMT has been successfully applied to information systems and cybersecurity contexts, demonstrating its relevance to privacy-protective behavior (Protection Motivation Theory in Information Systems Security Research, 2021; Shiri et al., 2024; Latent privacy management profiles, 2025). Studies consistently emphasize that educational institutions are responsible for safeguarding increasingly complex forms of student data, including academic records, behavioral analytics, and digital learning information (Nottingham et al., 2022; Correia de Barros & Vilela, 2025). Faculty members play a critical role because their daily decisions directly affect privacy outcomes. Effective data protection is associated with higher awareness, training, transparency, informed consent, and responsible data handling practices (Torres-Hernández & Gallego-Arrufat, 2023; Correia de Barros & Vilela, 2025). Institutions complement these efforts through governance structures, privacy policies, secure infrastructures, professional development programs, and continuous compliance monitoring (Nottingham et al., 2022; EDUCAUSE, 2022). The shift from paper-based to digital systems has improved efficiency but introduced new risks related to cyberattacks, unauthorized access, cloud vulnerabilities, and data breaches, requiring technical safeguards such as encryption, access controls, multi-factor authentication, and regular audits (OECD, 2023; Nawusu et al., 2024; Yakubu et al., 2024; Kapoh et al., 2024).

1.3 Local, National, and Global Context of Educational Data Privacy

Globally, educational institutions continue to face challenges in translating privacy regulations into operational practice. Studies report difficulties related to procedural compliance, risk management, staff awareness, and implementation consistency despite the presence of formal legal frameworks (Bowyer et al., 2022; Issaoui, 2023; Martius & Höchli, 2025; Turgut, 2022). Nationally, the Data Privacy Act of 2012 provides the legal framework for educational data protection in the Philippines through principles of transparency, legitimate purpose, and proportionality (National Privacy Commission [NPC], 2022; Respicio, 2025). Schools are required to appoint Data Protection Officers, establish safeguards, publish privacy notices, and report breaches when necessary (Martirez, 2023; Sancon, 2023; Tupaz, Candelario, & Unarce, 2025). Local studies indicate that awareness and compliance remain inconsistent across educational institutions. Faculty, students, and staff often demonstrate varying levels of understanding and application of privacy principles, while limitations in training, infrastructure, and institutional support continue to hinder compliance efforts (Ramos, 2022; Ayop et al., 2025; Canada et al., 2025; Alejandrino, 2024; Agup, 2024; Baluis, 2023).

1.4 Theoretical and Conceptual Basis of Faculty Data Protection Behavior

This study is anchored in the Protection Motivation Theory (PMT) of Rogers (1975), revised in Rogers (1983). PMT explains protective behavior through threat appraisal and coping appraisal. Threat appraisal consists of perceived severity and perceived vulnerability, while coping appraisal includes response efficacy, self-efficacy, and response cost. These cognitive evaluations influence protection motivation, which subsequently leads to protective behavior. Applying PMT to educational settings allows examination of faculty members' perceptions of data privacy threats, confidence in implementing privacy measures, and perceived barriers to compliance. Guided by these constructs, the study investigates faculty practices, challenges, and perceptions as the basis for developing a Data Protection Strategic Action Plan for NU Fairview.

1.5 Research Gaps and Rationale

Existing literature demonstrates that legal frameworks, institutional policies, and technical safeguards are essential for effective data protection. However, studies consistently report gaps between regulatory compliance and actual implementation within educational settings (Bowyer et al., 2022; Issaoui, 2023; Martius & Höchli, 2025; Ramos, 2022). Research further indicates that awareness alone does not guarantee privacy-compliant behavior, as faculty and students continue to engage in risky data practices despite understanding privacy principles (Ayop et al., 2025; Canada et al., 2025). Although previous studies have examined privacy awareness, compliance, and institutional governance, limited research has focused specifically on the implementation of data protection among Senior High School faculty in private educational institutions. This study addresses this gap by exploring faculty practices, challenges, and perceptions and by developing a context-specific Data Protection Strategic Action Plan for NU Fairview.

1.6 Alignment with Relevant Sustainable Development Goals (SDGs)

This study aligns primarily with SDG 4: Quality Education by promoting secure, ethical, and responsible management of educational information systems that support safe learning environments. It also supports SDG 16: Peace, Justice and Strong Institutions through the strengthening of institutional accountability, data governance, transparency, and compliance with privacy regulations. The study further contributes to SDG 9: Industry, Innovation and Infrastructure by encouraging secure digital transformation and responsible adoption of educational technologies while maintaining data protection standards.

1.7 Importance of the Study to Multidisciplinary Sustainability

The study contributes to educational sustainability by promoting responsible management of student information and strengthening institutional trust. It supports institutional sustainability through improved governance structures, policy implementation, and privacy compliance mechanisms. Additionally, the research contributes to technological sustainability by encouraging secure digital practices and data management systems. From a socio-economic perspective, protecting personal information minimizes risks associated with data breaches, strengthens stakeholder confidence, and promotes a culture of accountability and ethical responsibility within educational institutions. Ultimately, the proposed Data Protection Strategic Action Plan supports the long-term sustainability of educational operations, digital governance, and information security at NU Fairview.

2. Material and methods

2.1 Research Design

The study utilized a convergent parallel mixed-methods design, wherein quantitative and qualitative data were collected and analyzed during the same phase and subsequently integrated for interpretation (Creswell & Creswell, 2018). Following the Merging Data approach of Creswell and Plano Clark (2018), both datasets were given equal importance and examined independently before convergence. The integration process was facilitated through a Joint Display Method, which enabled a side-by-side comparison of quantitative and qualitative findings (Fetters et al., 2013). The quantitative component assessed faculty perceptions regarding data threats and their efficacy in protecting student information through a researcher-made survey, while the qualitative component explored faculty experiences, practices, and challenges through interviews and focused discussions. Deductive Thematic Analysis based on Braun and Clarke (2006) was employed to organize qualitative findings into themes aligned with the core constructs of Protection Motivation Theory (PMT). The integrated analysis provided the foundation for developing a context-specific Data Protection Strategic Action Plan.

2.2 Locale of the Study

The study was conducted at the Senior High School Department of NU Fairview during the Academic Year 2024–2025. The research focused on the implementation of data protection practices within the department, allowing for a localized assessment of how institutional privacy policies are translated into classroom and administrative workflows. Restricting the study to the Fairview campus ensured that the findings reflected the specific operational realities and data-handling culture of the institution.

2.3 Respondents of the Study

The respondents consisted of 45 full-time Senior High School faculty members who had served the institution for more than one academic year. This criterion ensured that participants possessed sufficient institutional knowledge and experience with both digital and physical data-handling procedures. Part-time faculty members were excluded because of their limited involvement in long-term administrative functions and institutional data management activities. The selected participants represented those most directly engaged in the institution's data processing lifecycle.

2.4 Sample and Sampling Procedure

The study employed purposive sampling to select participants who could provide informed insights regarding institutional data protection practices. Faculty members were chosen based on their tenure and active involvement in academic and administrative processes. For the quantitative phase, surveys were distributed to 45 qualified faculty members, of whom 44 completed the instrument. For the qualitative phase, eight faculty representatives, each representing a distinct learning area, participated in a Focus Group Discussion (FGD). This sampling strategy ensured that the perspectives gathered reflected diverse experiences while remaining grounded in the institution's operational realities.

2.5 Research Instrument

Two research instruments were utilized to address the study objectives. The quantitative component employed a Researcher-Made Protection Motivation Appraisal Survey designed to measure faculty perceptions related to Threat Appraisal, including perceived severity and vulnerability, and Coping Appraisal, including self-efficacy and response

efficacy. The instrument used a Likert-scale format and underwent expert validation by specialists in educational management and information technology to ensure alignment with the theoretical constructs of Protection Motivation Theory. The qualitative component utilized a Semi-Structured Interview Guide to explore faculty practices and challenges related to data protection. Through open-ended questions, participants described their experiences, perceived barriers, risky behaviors, and institutional gaps affecting compliance. The combination of both instruments allowed the study to examine perceptions, practices, and challenges comprehensively, providing a stronger foundation for the development of the proposed Data Protection Strategic Action Plan.

2.6 Data Gathering Procedure

Data collection commenced in March 2026 following the approval of the research proposal by the Senior High School Principal, Campus Research Coordinator, Academic Director, and Data Privacy Officer. The research instruments were submitted to expert validators and subsequently pilot-tested among eight faculty members using Microsoft Forms. Reliability testing was conducted using Cronbach's Alpha, and necessary revisions were implemented until an acceptable reliability coefficient of 0.70 was achieved. In April 2026, the quantitative survey was administered electronically to 45 eligible faculty members. The digital platform required informed consent before participation and incorporated privacy safeguards throughout the process. Forty-four completed responses were obtained. The qualitative phase was conducted in May 2026 through an online Focus Group Discussion facilitated via Microsoft Teams. Eight faculty representatives participated in a 1-hour and 10-minute discussion guided by the validated interview protocol. Prior to participation, all respondents signed consent forms authorizing their involvement and the recording of the session. Following data collection, recordings were transcribed using Microsoft Teams' automated transcription feature and manually verified for accuracy. The qualitative data were then analyzed using Deductive Thematic Analysis based on Braun and Clarke (2006). Finally, quantitative and qualitative findings were merged through a Joint Display Method, allowing direct comparison, convergence, and triangulation of results. The narrative explanation corresponding to the study's integration framework shows that quantitative findings regarding faculty perceptions were systematically compared with qualitative themes on practices and challenges to establish a comprehensive basis for the proposed Data Protection Strategic Action Plan.

2.7 Data Analysis Techniques

Quantitative and qualitative data were analyzed separately before integration. For the quantitative strand, descriptive statistics were used to determine faculty perceptions regarding data protection. Mean and standard deviation values were computed for the constructs of Threat Appraisal, including severity and vulnerability, and Coping Appraisal, including self-efficacy and response efficacy. The Weighted Mean was used to determine overall motivation levels and categorize respondents according to predetermined interpretation scales. For the qualitative strand, thematic analysis was employed. Recorded discussions were transcribed, coded, and organized into themes representing faculty practices, implementation gaps, and operational challenges. Thematic findings provided contextual explanations for the quantitative results and highlighted factors influencing compliance behaviors. The final stage involved triangulation through data integration. Quantitative findings were compared with qualitative themes to identify areas of convergence, divergence, and expansion. This merged analysis enabled the identification of gaps between institutional policies and actual faculty practices and served as the primary evidence base for developing the proposed Data Protection Strategic Action Plan.

2.8 Ethical Considerations

The study adhered to ethical principles throughout the research process. Informed consent was obtained from all participants after providing detailed information regarding the study's objectives, procedures, risks, benefits, and voluntary nature of participation. Participants were informed of their right to withdraw at any stage without consequence. Confidentiality was maintained through the use of pseudonyms and alphanumeric codes to protect participant identities. All survey responses, focus group discussions, and related materials were anonymized and securely managed. Participation was entirely voluntary, and respondents were assured that their involvement would not affect their employment, professional relationships, or performance evaluations. To ensure credibility and trustworthiness, the instruments underwent expert validation and reliability testing. Data triangulation was achieved through the Merging Approach, wherein quantitative and qualitative findings were compared to validate interpretations. Member-checking was also conducted by allowing participants to review summaries of the discussions and verify the accuracy of the recorded information. These procedures strengthened the reliability, validity, and ethical integrity of the research process.

3. Results and Discussion

3.1 Data Protection Practices of Senior High School Faculty

3.1.1 Physical Data Protection Practices

The findings indicate that faculty members consistently apply physical data protection measures in their daily workflows. Common practices include covering student information during grade verification, storing records in secure folders and containers, and minimizing the inclusion of sensitive information in classroom materials. These practices demonstrate efforts to prevent unauthorized disclosure of student information and maintain confidentiality. These practices reflect

strong awareness of the risks associated with physical records and demonstrate adherence to principles of confidentiality and data minimization. The findings support the observations of Njoku and Njoku (2025), Yakubu et al. (2024), Torres-Hernández and Gallego-Arrufat (2023), Respicio (2025), and the National Privacy Commission (2022), which emphasize the importance of safeguarding sensitive educational records and limiting unnecessary collection of personal information.

3.1.2 Digital Data Protection Practices

Faculty members reported implementing various digital safeguards, including reviewing access permissions before sharing files, restricting access to authorized users, utilizing separate cloud storage systems, and removing folder permissions after the completion of academic terms. These practices indicate deliberate efforts to secure digital records and prevent unauthorized access. The findings demonstrate that faculty recognize the importance of access control and secure file management. These practices align with the recommendations of Mollakuqe and Dimitrova (2024), UNICEF (2024), Correia de Barros and Vilela (2025), and Kapoh et al. (2024), which emphasize controlled access, secure storage, and responsible management of educational data. Despite institutional limitations, faculty members continue to adopt adaptive strategies to maintain compliance.

3.1.3 Communication and Preventive Safeguarding Practices

The findings show that faculty avoid sharing individual student information through public communication channels. Instead, they communicate aggregated performance data and restrict sensitive information to institutional platforms. Some faculty members also avoid collecting unnecessary personal information and practice secure disposal of documents containing sensitive data. These behaviors demonstrate attempts to balance operational efficiency with privacy protection. The findings support the arguments of Ayop et al. (2025), NPC (2022), Kapoh et al. (2024), Correia de Barros and Vilela (2025), Njoku and Njoku (2025), and Yakubu et al. (2024), which highlight the importance of data minimization, responsible communication practices, and secure disposal procedures in preventing privacy violations.

3.2 Challenges and Response Costs in Implementing Data Protection

3.2.1 Infrastructure and Resource Constraints

Faculty members identified inadequate cloud storage capacity and limited physical storage facilities as major barriers to data protection implementation. Several participants reported purchasing personal cloud subscriptions to compensate for institutional limitations, while others noted insufficient physical storage spaces for sensitive documents. These findings suggest that resource limitations increase the cost of compliance and place additional burdens on faculty. The results support the findings of Miano (2025) and King and Pajo (2025), which identify inadequate infrastructure and resource constraints as persistent barriers to data privacy compliance. The situation also reflects concerns raised by Gundaboina (2025), OECD (2023), Njoku and Njoku (2025), and Yakubu et al. (2024) regarding the importance of adequate digital and physical infrastructure for effective data protection.

3.2.2 Operational Friction and Compliance Burdens

Participants reported that compliance requirements such as file-formatting standards, uploading procedures, and multi-factor authentication increase workload and occasionally delay task completion. While these safeguards were generally accepted, they were also perceived as sources of inconvenience during periods of heavy academic responsibilities. The findings indicate that security controls can create operational burdens when not adequately supported by institutional systems. This observation aligns with Kapoh et al. (2024) and Anderson and Choong (2023), who emphasize that technical safeguards often generate user friction when implementation is not balanced with practical workflow considerations.

3.2.3 Knowledge Gaps and Policy Dissemination Issues

Faculty members expressed limited familiarity with institutional privacy statements and reported that data privacy policies were often communicated superficially rather than translated into practical workplace procedures. As a result, some participants relied on personal interpretations and self-developed workarounds to maintain compliance. These findings suggest that awareness of data privacy regulations does not necessarily translate into operational competence. The results support Ramos (2022) and Martius and Höchli (2025), who argue that institutions frequently struggle to transform regulatory requirements into actionable workplace practices. The findings also reinforce concerns regarding inadequate privacy training and policy implementation in educational settings.

3.2.4 Physical and Digital Workplace Vulnerabilities

Faculty members reported challenges related to open workspaces, exposed documents, and occasional reliance on personal communication channels for professional interactions. These situations created opportunities for accidental disclosure and blurred the boundaries between personal and institutional data environments. The findings highlight how environmental conditions and convenience-driven behaviors can weaken data protection efforts. These observations support the findings of Sancon (2023), Ayop et al. (2025), Njoku and Njoku (2025), and Baluis (2023), which emphasize that inadequate controls and workplace practices increase exposure to privacy risks.

3.3 Faculty Perceptions of Data Threats and Efficacy in Safeguarding Information

3.3.1 Perceived Severity and Vulnerability of Data Threats

Survey findings revealed a high level of agreement among faculty regarding the seriousness of data breaches and the vulnerability of student information. Respondents recognized that failure to follow established protocols could result in unauthorized access, reputational damage to the institution, and negative consequences for students. Faculty also acknowledged the importance of institutional security measures and compliance with digital protocols. These findings indicate a strong threat appraisal among faculty members. Their awareness of data security risks reflects a clear understanding of the consequences associated with privacy violations and supports the central assumptions of Protection Motivation Theory regarding perceived severity and vulnerability as drivers of protective behavior.

3.3.2 Perceived Self-Efficacy and Response Efficacy

Faculty generally expressed confidence in their ability to follow data protection procedures, identify suspicious communications, and apply data minimization principles. However, confidence was comparatively lower regarding technical competencies and formal reporting procedures for privacy incidents. These findings suggest that faculty possess strong confidence in routine protective behaviors but may require additional support in technical and procedural areas. The results indicate that self-efficacy is strongest in everyday classroom practices and weaker in specialized security-related functions, highlighting areas for capacity-building and training.

3.3.3 Perceived Barriers to Compliance

Faculty reported a generally neutral perception regarding the burden of data protection requirements. While some respondents viewed privacy compliance as manageable, others perceived additional workload, technical demands, and changing mandates as significant challenges. The findings also revealed substantial variation in responses, indicating differing experiences across participants. The variation in responses suggests that operational barriers are not experienced uniformly across the faculty. While some educators adapt effectively to privacy requirements, others face greater difficulty due to workload, technological demands, or resource limitations. This finding reflects the role of response costs within Protection Motivation Theory and demonstrates how perceived burdens can influence compliance behavior.

3.4 Convergence of Quantitative and Qualitative Findings

The integrated analysis revealed strong convergence between quantitative and qualitative findings regarding faculty awareness of data risks. Faculty consistently recognized the vulnerability of student information and the consequences of non-compliance. Qualitative narratives further confirmed concerns about exposed documents, inappropriate use of social media, and insufficient policy implementation. At the same time, qualitative findings revealed that many reported compliance behaviors were supported by self-developed workarounds rather than formal institutional guidance. Faculty also described infrastructure limitations that affected their ability to fully implement data protection measures. The convergence analysis demonstrates that faculty possess high awareness of data protection risks but face significant organizational and infrastructural barriers. While quantitative results suggest strong confidence in routine compliance behaviors, qualitative findings reveal that such confidence often depends on compensatory strategies developed to address policy ambiguities and resource limitations. These findings indicate a gap between institutional expectations and operational realities, reinforcing the need for stronger support systems, clearer procedures, and improved infrastructure to sustain effective data protection practices.

3.5 Proposed Data Protection Strategic Action Plan

The findings indicate that faculty possess strong motivation to protect student information but face limitations related to infrastructure, policy implementation, training, and operational efficiency. The proposed Data Protection Strategic Action Plan focuses on expanding secure storage resources, improving physical and digital infrastructure, strengthening policy dissemination, enhancing technical and privacy-related training, and reducing procedural barriers that discourage compliance. The proposed interventions align with Protection Motivation Theory by reducing response costs while improving self-efficacy and response efficacy. Consistent with the recommendations of Rogers (1975, 1983, as cited in Shiri et al., 2024), Issaoui (2023), Martius and Höchli (2025), Kapoh et al. (2024), UNICEF (2024), Sancon (2023), and NPC (2022), strengthening institutional support mechanisms can help transform faculty awareness into sustained, compliant, and ethical data protection practices.

4. Conclusion and Recommendations

The study found that Senior High School faculty possess a strong awareness of data protection risks and recognize the importance of safeguarding student information. Faculty members actively implement physical and digital protective practices; however, these efforts are often driven by self-developed workarounds rather than standardized institutional procedures. Despite high levels of threat awareness and motivation to protect data, compliance is hindered by limited policy

dissemination, inadequate technical guidance, insufficient cloud and physical storage resources, and operational burdens associated with existing security requirements. As a result, faculty members frequently compensate for institutional limitations through personal initiatives, creating inconsistencies in data protection practices. The findings indicate that strengthening institutional support, infrastructure, and practical implementation mechanisms is necessary to translate awareness into consistent and sustainable compliance.

The university should formally implement the proposed Data Protection Strategic Action Plan and allocate the necessary resources to strengthen data protection practices. This includes expanding official cloud storage capacity, improving physical storage facilities, providing practical and clearly communicated data privacy procedures, and offering continuous training focused on technical skills and reporting processes. Security requirements should be reviewed to minimize unnecessary operational delays while maintaining compliance. Faculty members should consistently utilize approved institutional platforms for storing and sharing information and actively participate in privacy training activities. Students should remain mindful of their personal information and use formal reporting channels when privacy concerns arise. Future studies may examine the long-term effects of the Strategic Action Plan and explore data privacy practices among other educational stakeholders and campuses.

The study was limited to full-time Senior High School faculty members of NU Fairview who had served the institution for more than one academic year. It was confined to a single campus and focused only on faculty perceptions, practices, challenges, and protection motivation related to data protection. Part-time faculty, students, administrators, and personnel from other campuses and educational levels were not included. The findings therefore reflect the specific operational context of the NU Fairview Senior High School Department and may not fully represent the experiences of other institutions, campuses, or stakeholder groups.

Compliance with ethical standards

The author declares no conflict of interest. This study received no external funding and was conducted with the cooperation of National University Fairview and its participating Senior High School faculty members. Participation was voluntary, and informed consent was obtained from all participants prior to data collection through non-invasive methods, including surveys and focus group discussions. All responses were anonymized, and no identifying information was disclosed to ensure participant confidentiality and protect privacy throughout the research process.

REFERENCES

- Agup, A. P. (2024). Data Privacy Act: Awareness, compliance, and challenges of nurses of government hospitals in Northern Philippines. *Philippine Social Science Journal*, 7(2), 112–122.
- Alejandrino, L. M. (2024). An analysis of state universities and colleges students' level of awareness on digital footprints and data privacy in Davao Region, Philippines. *International Journal of Multidisciplinary: Applied Business and Education Research*, 5(4), 1258–1269.
- Almekhled, A., & Petrie, H. (2024). University academics' awareness and knowledge of online privacy and security policies: A mixed-methods study. *Education and Information Technologies*, 29(2), 1187–1204.
- Anderson, M., & Choong, Y.-Y. (2023, October 10). *Using strong passwords and a password manager* [Blog post]. NIST Computer Security Resource Center.
- Asia-Pacific Economic Cooperation. (2015). *APEC privacy framework*. [https://www.apec.org/publications/2017/08/apec-privacy-framework-\(2015](https://www.apec.org/publications/2017/08/apec-privacy-framework-(2015)
- Asian Journal of Management Studies. (2021). *Assessment of the implementation of the Data Privacy Act of 2012 (RA 10173) in higher educational institutions*. <https://asianjournals.org/online/index.php/ajms/article/download/459/275/1283>
- Ayop, J. R., Larecion, R. C., Respulo, A. A. P., Villasureda, R. A. S., Arendain, K. M. A., & Cantil, J. B. J. (2025). Relationship of social media usage and data privacy awareness among college students in the municipality of Bansalan. *Asian Journal of Education and Social Studies*, 51(7), 617–627.
- Baluis, M. J. (2023). Safeguarding privacy, ensuring ethics: Exploring implications of data-driven workforce planning in state universities and colleges. *Philippine Journal of Educational Management*, 30(1), 45–60.
- Canada, J. R., Lara, A., Jr., Josol, C., & Albon, E. (2025). Online privacy concerns, impacts and coping strategies among college students in Digos City, Philippines: A descriptive phenomenological study. *Asian Journal of Education and Social Studies*, 51(10), 605–619.
- Correia de Barros, Y., & Vilela, J. (2025). Data privacy in educational contexts: Analyzing perceptions, practices and challenges in personal data protection. *Contemporary Educational Technology*, 15(1), ep399.
- Dalelio, C. M. (2024). Respecting students' privacy boundaries and media use preferences while teaching with online digital tools. *Journal of Public Relations Education*, 10(3), 158–177.

- de Barros, P. M., & Vilela, R. S. (2025). Data protection practices and challenges in Brazilian educational institutions under the LGPD: A case-based analysis. *Journal of Information Privacy and Security*, 21(1), 33–52.
- EDUCAUSE. (2022). *Student data privacy and security: A call for transparent practices*. EDUCAUSE.
- General Data Protection Regulation. (2018). *What is GDPR, the EU's new data protection law?* <https://gdpr.eu/what-is-gdpr/>
- Gundaboina, A. K. (2025). Securing BYOD (Bring Your Own Device) in education: Endpoint management for school networks. *Journal of Engineering and Applied Sciences Technology*, 7(4), 1–6.
- Hahn, A. (2024). *Communication Privacy Management Theory*. EBSCO Research Starters.
- Halawi, L. A., & Makwana, A. (2023). GDPR compliance in U.S. higher education institutions: A comparative review and implications for data governance. *Journal of Higher Education Policy and Management*, 45(4), 437–456.
- Halawi, L., & Makwana, A. (2023). The GDPR and UK GDPR and its impact on US academic institutions. *Issues in Information Systems*, 24(2), 232–241.
- International Organization for Standardization. (2019). *ISO/IEC 27701:2019 Security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management—Requirements and guidelines*. <https://www.iso.org/standard/71670.html>
- Kapoh, H., Aprilyana, P., Sumampow, Y. J. R., Mailake, M. P., Manimpurung, F. H., & Pakaya, H. Q. (2024). Data security and data protection in cloud privacy systems. *Jurnal Syntax Admiration*, 5(11), 4801–4809.
- King, E. M. N., & Pajo, P. (2025). *AI in Philippine education: Opportunities, challenges, and ethical considerations for personalized learning* [Preprint]. ResearchGate.
- Lu, H., Wei, A., & Li, X. (2025). Understanding the privacy disclosure behavior and privacy concerns on short-form video platforms: An empirical investigation. *Frontiers in Psychology*, 16, 1535533.
- Mailok, R., Nordin, N., & Sulaiman, A. (2023). University students' awareness and practices of personal data protection in Malaysia. *International Journal of Advanced Computer Science and Applications*, 14(5), 456–463.
- Martirez, K. C. (2023). Compliance on Data Privacy Act of private higher educational institutions in the province of Albay: Basis for information governance model. *International Journal of Education, Business and Economics Research*, 3(3), 26–36.
- Miano, L. C. (2025). Awareness on data privacy vis-à-vis data management practices at a state university in Quezon province: Input towards data-driven policy and manual for good governance. *Edelweiss Applied Science and Technology*, 9(1), 302–315.
- Mollakuqe, E., & Dimitrova, V. (2024). Comparative analysis of identity management, access control, and authorization practices in public and private universities. *Open Research Europe*, 4, Article 23.
- National Privacy Commission. (2020). *Advisory No. 2020-01: Guidelines on the use of videoconferencing tools and similar applications in the education sector*. <https://privacy.gov.ph/wp-content/uploads/2023/05/DP-Council-Education-Sector-Advisory-No.-2020-1.pdf>
- National Privacy Commission. (2022, March 25). *Privacy Policy Office Advisory Opinion No. 2022-014: Recording and uploading of online classes* [PDF]. National Privacy Commission.
- National Privacy Commission. (n.d.). *Breach reporting*. National Privacy Commission.
- National University. (2023). *Faculty manual 2023*.
- National University. (2024). *Privacy policy*. <https://www.national-u.edu.ph/privacy/>
- National University. (2025, May 19). *NU campuses unite for basic research ethics training – Batch 2*. <https://www.national-u.edu.ph/nu-laguna/nu-campuses-unite-for-basic-research-ethics-training-batch-2/>
- Nottingham, E., Stockman, C., & Burke, M. (2022). Education in a datafied world: Balancing children's rights and schools' responsibilities in the age of COVID-19. *Computer Law & Security Review*, 45, 105664.
- Parents' perceptions of privacy policies and practices for school-issued digital devices: Implications for school practices*. (2022). *PLOS ONE*, 17(9), e0274667.
- Ramos, G. L. (2022). Perceptions of students, faculty, and administrative staff on the Data Privacy Act: An exploratory study. *Asia Pacific Journal of Multidisciplinary Research*, 10(3), 34–46. <https://doi.org/10.5281/zenodo.7654981>
- Republic Act No. 10173. (2012). *The Data Privacy Act of 2012*. <https://privacy.gov.ph/data-privacy-act/>
- Respicio, H. (2025, April 30). *Data privacy for student grades in the Philippines: A comprehensive legal primer (updated 30 April 2025)*. Respicio & Co. Law Firm.
- Sancon, R. J. S. (2023). Data privacy best practices of a local higher educational institution: A model for governance. *IOER International Multidisciplinary Research Journal* (Special Issue, June 2023), 9–16.
- Torres-Hernández, N., & Gallego-Arrufat, M.-J. (2023). Pre-service teachers' perceptions of data protection in primary education. *Contemporary Educational Technology*, 15(1), ep399.
- Tupaz, E. F., Candelario, L. R., & Unarce, J. S. (2025, February 20). *Philippines: The NPC's advisory on child-oriented transparency*. Gorriceta Africa Cauton & Sia.
- UNICEF. (2024). *Data protection in schools: Guidance for legislators, policy makers and schools*. UNICEF Regional Office for Europe and Central Asia.
- Wiefeling, S., Janson, A., & Thielsch, M. T. (2023). Challenges in implementing GDPR-compliant data management: Insights from data protection officers in large organizations. *Information Systems Frontiers*, 25(3), 589–610.