International Journal of Management, Knowledge and Learning | ISSN 2232-5697

Data Protection in Pre-Tertiary Schools in Ghana

Elizabeth Serwaah Baah
University of Education, Winneba
220027883@st.uew.edu.gh

Ephrem Kwaku Kwaa Aidoo
University of Education, Winneba
ekkaidoo@uew.edu.gh

Purpose: The study examines data protection practices in pre-tertiary schools in Ghana, specifically focusing on compliance with the Data Protection Act, 2012 (Act 843).

Study design/methodology/approach: It adopts a mixed-method approach, surveying representatives from one hundred schools and interviewing representatives from sixteen schools and two education offices. Respondents were staff assigned to manage school data from three strata: the basic school level, senior high school level, and the Ghana Education Service.

Findings: The findings reveal a general awareness of data protection laws among staff handling and managing data. However, it also uncovers a significant gap in their understanding of principles and legal obligations. The study also identifies a lack of coordination, formal guidance, inadequate consent procedures, and fragmented implementation strategies in data protection practices. Furthermore, the use of varied data protection mechanisms by different schools suggests a lack of standardised security protocols, which is likely to result in security gaps. This is particularly noteworthy considering the frequent data transfers and the challenging data protection environment that combines physical and digital storage methods in potentially unsecured locations across multiple schools.

Originality/value: The findings can contribute to developing a standardised data protection policy for Ghanaian pre-tertiary schools, enhanced employee training, and increased awareness to ensure effective compliance and protection of personal data in Ghana's pre-tertiary education system, thereby mitigating potential risks of data breaches and privacy violations.

Keywords: Data Protection, Cyber Security, Privacy, Pre-tertiary schools

1 Introduction

In recent years, the digital transformation of educational institutions has led to the widespread collection, storage, and processing of personal data, raising concerns about data protection and privacy. (Limba & Šidlauskas, 2020)The way societies generate, process, and disseminate personal data has changed dramatically due to the global integration of information systems, forcing countries to reevaluate and strengthen their data protection laws and mechanisms.

Like other nations, Ghana has witnessed a rapid evolution of its information ecosystem and technology advancement, especially in the education sector, making it a compelling case study in the dynamics of data governance. As pre-tertiary schools in Ghana increasingly rely on digital technologies for administrative, instructional, and communication purposes, understanding their data protection practices and compliance with relevant regulations becomes paramount. The Ghana Education Service has introduced various IT systems into the school system. These include the Educational Management Information System (EMIS), various learning management platforms, including the iBox/iCampus, Computerised School Selection and Placement Systems (CSSPS), and the School Information Systems. This is in addition to other school-based student records and learning management platforms. The Central and Western regions of Ghana, known for their long and diverse history in the Ghanaian

educational landscape, present a valuable context for examining the status of data protection practices in pre-tertiary schools.

2 Purpose of the Study

An analysis of Verizon's data breach investigation report of 2018 revealed that the most common compromised information assets are personal information. This is particularly true for the education sector, as shown in Table 1 where the most compromised information asset is personal data and constitutes 72% of compromised assets. Though such statistics are not available for Ghanaian institutions, there is no doubt that data protection should be a primary goal of educational institutions.

Table 1: Industries and their most Compromised Information Assets

Economic Sector	Most Compromised Assets	Percentage of breaches
Accommodation and food services	Payment	93%
Education	Personal	72%
Financial and insurance	Personal	36%
Health care	Medical	79%
Information	Personal	56%
Manufacturing	Personal	32%
Professional, technical and Scientific Services	Personal	57%
Public Administration	Personal	41%
Retail	Payment	73%

Source: (Berinato & Perry, 2019)

Education is undoubtedly a substantial sector in the Ghanaian economy, especially since most of the Ghanaian population is young and likely to be in school. School enrolment statistics retrieved from the UNESCO Institute of Statistics are shown in Table 2 below.

Table 2: Pre-tertiary Enrolment Statistics of Ghana

Level	Enrolment
Pre-primary:	1,608,388
Primary:	4,431,837
JHS & SHS/TVI:	3,885,855
Total	**9,926,080**

Source: UNESCO Institute of Statistics

With a population of about 30 million Ghanaians, the pre-tertiary education sector covers over 30% of the country's population. Therefore, data privacy or protection must be rigorously implemented in the pre-tertiary space.

Several factors underscore the importance of investigating data protection practices in pre-tertiary schools in Ghana. Firstly, Ghana's Data Protection Act, 2012 (Act 843) mandates organisations, including educational institutions, to adhere to principles and standards for legally processing personal data (Parliament of Ghana, 2012). However, the extent to which pre-tertiary schools in Ghana comply with these regulations remains largely unexplored. Secondly, the proliferation of digital platforms and online learning systems in schools introduces new risks related to data breaches, unauthorised access, and misuse of personal information. Understanding the readiness of schools to address these risks through robust data protection measures is essential for safeguarding the privacy rights of students, parents, and staff members.

Moreover, the research also considers the broader socio-economic and cultural context within which pre-tertiary schools operate. Factors such as varying levels of technological infrastructure, resource constraints, and awareness about data protection practices may influence the implementation of data protection measures across different schools.

The main objective of the study was to investigate the nature of data management and the extent to which data protection practices have been implemented in pre-tertiary schools to comply with the law. It also examines the mechanisms employed by pre-tertiary schools to achieve Data Protection Act compliance.

3 The Goals of Data Protection

Data Protection is based on several basic principles that guide the processing of personal data. These principles aim to ensure that the rights of data subjects are protected and that their data are processed fairly, transparently and by the law.

The legal framework relating to data protection in education, particularly in the U.S., places significant responsibility on institutions to comply with data protection regulations. The Family Educational Rights and Privacy Act (FERPA) mandates that schools implement measures to safeguard student information (Sinan et al., 2024). Such regulations underscore the necessity for developing tailored, robust security solutions in educational contexts, extending to the implementation of information security awareness programs that could significantly improve stakeholder understanding of data protection (Runtuwene et al., 2019). In Ghana, there are no laws that specifically focus on data protection in schools. However, the Data Protection Act 2012 (Act 843) regulates all public and private organisations that collect and use personal information safeguarding individuals' privacy rights (Parliament of Ghana, 2012). The Act generally aligns with the principles of international data protection standards.

The UK Data Protection Act of 1998 was a landmark law that introduced the eight data protection principles based on the 1995 EU Data Protection Directive 95/46/EC, which was the precursor to the General Data Protection Regulation (GDPR) (European Parliament & Council of the European Union, 1995, 2016). A comparison of the principles that the three laws seek to achieve has been made below.

Table 3: Comparison of Data Protection Laws

1998 Act	2012 Act 843	GDPR
Principle 1: fair and lawful	Accountability	Principle (a) – lawfulness, fairness and transparency
Principle 2: purposes	Lawfulness of processing	Principle (b) – purpose limitation
Principle 3: adequacy	Specification of purpose	Principle (c) – data minimisation
Principle 4: Accuracy	Compatibility of further processing with the purpose of collection	Principle (d) – accuracy
Principle 5: Retention	Quality of information	Principle (e) – storage limitation
Principle 6: rights	Openness	Principle (f) – integrity and confidentiality (Security)
Principle 7: Security	Data security safeguards	Accountability
Principle 8: International transfers	Data subject participation	

These principles indicated in Table 3 typically constitute the goals of any data protection system set up to comply with the regulation.

4 Achieving Data Protection

Implementing data protection is a shared responsibility involving oversight by senior management. A Data Protection Officer (DPO), as required by the Data Protection Act, 2012 (Act 843), ensures adherence to the law. IT security officers implement technical controls, while the legal and compliance teams develop privacy policies that ensure regulatory compliance.

In a digitised system, achieving data protection is fundamentally a cyber security issue (European Union Agency for Cybersecurity, 2019; National Institute of Standards and Technology 2018). Consequently, organisations incorporate their data protection measures into their cyber security strategy. This will typically include implementing technical controls such as access controls, encrypting data where necessary, and ensuring that all data is securely stored. Such controls are best implemented in a centrally managed information system that enforces policies across the entire organisation. This presupposes that organisations will have IT security policies. Encryption of data at rest and in transit in centrally managed systems ensures end-to-end protection. Password policies like complexity requirements and password expiration are also best enforced through centralised identity management systems. Automated software updates and patch management can also be done in a centrally managed system. Access control remains a critical strategy to prevent unauthorised access in the context of information security in educational settings that advocate for robust networks to secure against potential threats (Peng et al., 2022). Integrating advanced authentication methods, such as multi-factor authentication (MFA), is also critical for enhancing system access security in educational environments. Research indicates that implementing MFA can substantially reduce security vulnerabilities and bolster the integrity of educational information systems (Cahyaningrum, 2024).

Other studies have suggested that using emerging technologies, such as blockchain and artificial intelligence, presents opportunities to protect education data. Blockchain technology, for example, is cited as a potential means to enhance data security and transparency in educational processes (Samala et al., 2024) and that could potentially address data security and privacy goals (Delgado-von-Eitzen et al., 2024).

The first two principles in Table 3 cover the purpose of collection and the lawfulness of processing personal data. These two principles generally require providing the data subject with the purpose for which the data is being collected and obtaining explicit consent from the data subject. In a digitised system, technologies could be used to manage these. They include publishing the purpose in a terms and conditions document and consenting to these terms by checking a box or clicking a button to signify their consent. It must be emphasised that though regulation requires obtaining and managing meaningful consent, privacy is very complex, involves uncertainty, is context-dependence, and its interpretation is malleable (Acquisti et al., 2015; Schwartz & Solove, 2011). It raises various issues, including who gets to access personal data and the context in which such information is accessed. Such risks could be mitigated using administrative controls. Section 3.7 of the code of conduct for GES staff deals with access to and disclosure of privileged information (Ghana Education Service Council, 2017)

Maintaining accurate personal data is vital, and data controllers must take reasonable steps to ensure its accuracy and timeliness. However, Act 843 does not yet have specific requirements for data controllers to ensure data accuracy or mechanisms for individuals to correct inaccuracies. Though this is a weakness in the law, it requires data controllers to comply with the data protection legislation of a subject's foreign jurisdiction, particularly where personal data originating from that jurisdiction is sent to Ghana. With schools sometimes having

foreigners, they are obligated to have measures to handle such data when they collect them, though not directly required by Ghanaian law.

Various studies point to the complexity and multi-dimensional nature of Data protection. They have suggested that data protection has a complex and multi-dimensional nature involving technical measures, organisational policies, including data access policies and protocols, staff training and human factors (Smith et al., 2011; van der Aalst, 2016). Dealing with such complexity requires physical, technical, and administrative controls. The expectation is to have a multi-layered security solution allowing different controls to guard against whatever threats come to pass. This approach, referred to as defence in depth, proposes security solutions that are designed in layers such that a single failed control should not result in the exposure of systems or data (Chapple et al., 2021).

A study on compliance by organisations with GDPR found that large organisations and security-oriented small-to-medium organisations(SMEs/SMBs) generally found compliance reasonably achievable (Sirur et al., 2018). On the other hand, SMEs with limited security or data protection capabilities found it challenging to achieve satisfactory compliance. In Ghana, pre-tertiary schools comprise early grade, primary, junior, and senior high education. There are over 310 thousand teachers and 9 million learners in the pre-tertiary education sector under the Ghana Education Service (GES). The GES was established as part of the Public Service, with the responsibility to oversee all facets of pre-tertiary schools in Ghana and implement policies and programs to ensure that Ghanaian children of school-going age are provided with inclusive and equitable quality formal education. The GES also offers guidelines and standards to manage and facilitate effective teaching and learning (Ghana Education Service, ND).

Data infrastructure in schools and secure data storage systems present complex challenges. Schools' data infrastructures are characterised by ad hoc development, limited interoperability, and ongoing maintenance needs, complicating rather than simplifying institutional processes (Pangrazio et al., 2022) . This patchwork approach contrasts with fully centralised architectures and highlights the disjuncture between anticipated benefits and practical realities of data use in educational settings.

5 Methods

A mixed-method approach, combining quantitative and qualitative methods, was utilised in this study. As discussed earlier, data protection is socio-technical, complex and multifaceted; hence, it requires a research design that can explore the breadth of the issues and provide a general understanding but also give deeper insights, including contextual interpretations, perceptions of data protection and challenges in schools. It also offers an opportunity to triangulate the data, enhancing the validity and reliability of the findings (Creswell & Clark, 2018; Creswell & Creswell, 2018).

A stratified convenient sampling strategy was used to select a sample. This approach was chosen to reduce sampling error, enhance generalizability, and enable unbiased research results (Cochran, 1977). The population was split into three strata: basic school level, senior high school level, and GES. A snowball sampling technique was used to contact schools willing to participate in the study.

One hundred (100) schools were contacted and given questionnaires, and 84 schools completed the survey, giving a response rate of 84%. This comprises 83.3% of Basic schools contacted and 85% of Senior High Schools (SHS) contacted. For the qualitative phase, the study interacted with sixteen (16) schools from both basic and SHS strata, ten (10) from the basic level and six (6) from the SHS level. Two (2) GES offices and one (1) district office, each from the Central and Western regions, were selected for interviews. One staff member from each

sample school and office was interviewed or asked to complete the questionnaire on behalf of the school or office. The study focused on staff members because they are the primary handlers of personal data within schools. These staff members designated to oversee data collection and management were the respondents and are referred to as data managers in the study.

6 Results and Discussions

6.1 Data Collection and Handling

It was found that the pre-tertiary schools surveyed use various data collection processes, such as enrolment forms, student information systems, and online portals, to collect student information. Additional procedures, such as requesting supporting documents and conducting periodic data audits, were used to help verify the authenticity and accuracy of student data.

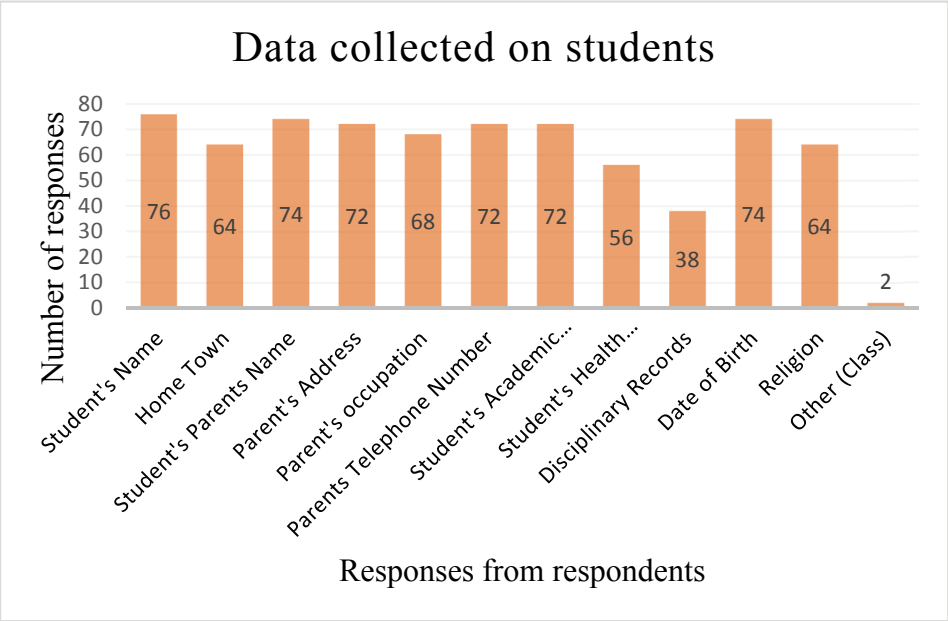

Figure 1: Types of Personal Data Collected

Figure 1 above shows the types of personal data collected by the schools surveyed.

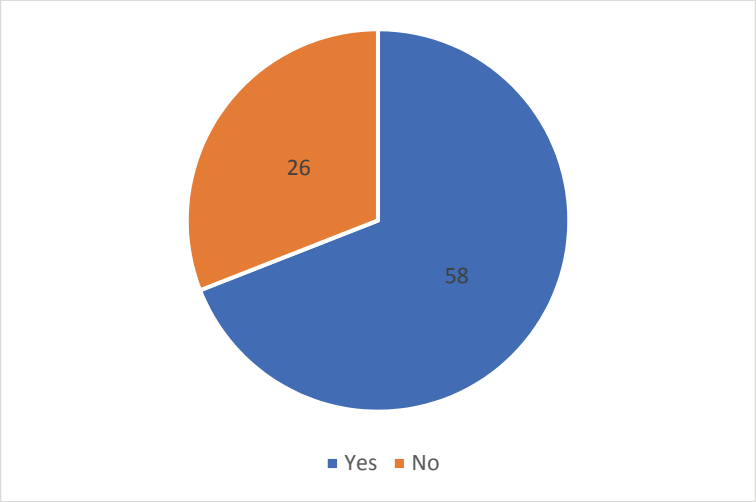

Figure 2: Consent Given by Data Subjects

On the question of whether data subjects give consent to their personal data being collected and used, 58 respondents, representing 69%, as shown in Figure 2 indicated that they obtained

consent from the data subjects and their parents when collecting this data. More than a quarter of respondents, however, indicated that they did not receive the consent of data subjects. It is worth noting that more than a quarter of respondents said they did not receive consent from data subjects before collecting their data. This suggests a significant gap in compliance with data protection standards and raises serious ethical and legal concerns. It could also lead to violations of privacy rights and expose the schools to legal risks.

Subsequent interviews, however, provided more context to the issue of consent, indicating that consent is assumed. All 16 data managers interviewed said that parents do not give explicit consent in written or any other form; once they complete admission forms, it is assumed that they had consented to their data being taken and used. One interviewee disclosed, "Parents and guardians of pre-tertiary students are required to accompany their wards during data collection, and their presence indicates consent to us. Additionally, students and staff are expected to provide necessary data for their benefit and organisational planning". Another interviewee pointed out, "Most parents have a sense of coercion during data collection and tend to provide data without realising they have the option to say no". The law and best practices require that data subjects give explicit consent, not assumed consent.

Interviews also indicated that the data collected is stored on the schools' premises. However, they also revealed that the data is shared with other organisations within the education space, as shown in the data life cycle in Figure 3 below.

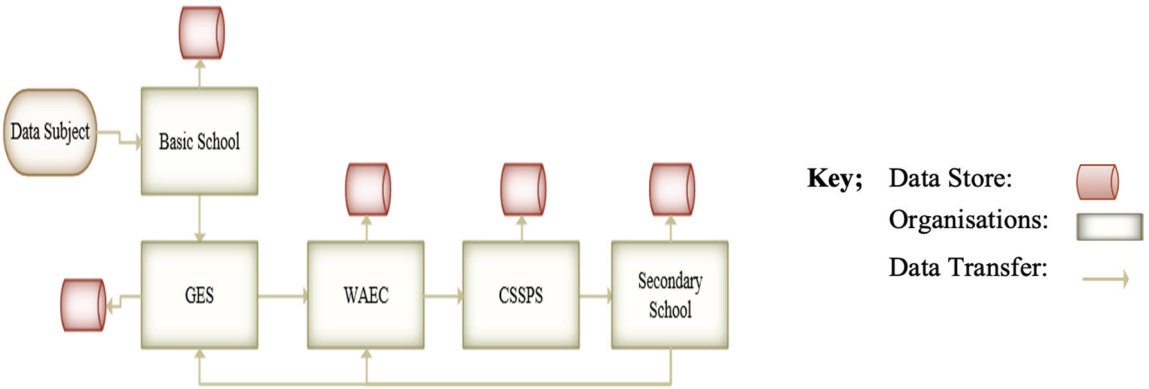

Figure 3: Data Lifecycle in the Pre-tertiary Educational System

This personal data sharing is typically done to facilitate various administrative processes, such as student registration for final examinations, placement into senior high schools and creation of user accounts to enable access to e-learning materials. While this inter-agency transfer is necessary to improve service delivery, it raises significant concerns about data privacy and security, especially if there is no strict guidance on the use of the data.

As per the law, such transfers are permitted if the data subject has given explicit consent to transfer their data to a third party. Consent must be informed, meaning the individual understands the purpose of the transfer, who will receive the data, and what protections are in place. This as indicated above does not happen.

6.2 Knowledge of Data Protection

Knowing about the law is help in complying with it. Figure 4 above shows that 56% of respondents know about Ghana's data protection law. This shows that most data managers

recognise that there is a law that governs the collection, use and protection of personal data in Ghana. This awareness is a positive indicator of the likelihood of complying with the law. On the other hand, a significant 44% of data managers reported having no knowledge of the existence of the law. This lack of awareness raises concerns, suggesting that nearly half of the staff responsible for managing sensitive data do not know about their legal responsibility to protect personal data. Additionally, when their knowledge was tested, 76% of the respondents were able to select the correct description of data protection; however, 24% of respondents picked the wrong definition.

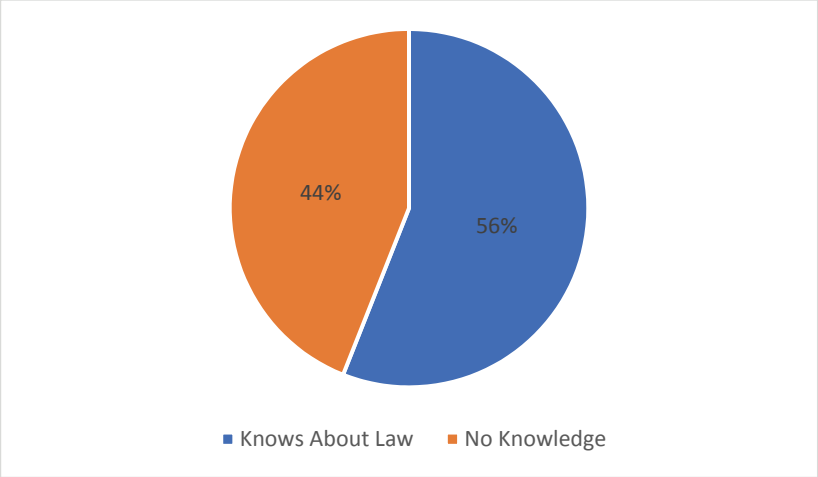

Figure 4: Staff Knowledge of Data Protection Law

The data suggests a concerning gap in awareness and understanding among data managers about a law critical to their work. This gap highlights the urgent need for schools to improve education and awareness around data protection laws to ensure all data managers are familiar with and comply with the law and help reduce potential risks associated with data breaches and non-compliance.

6.3 Implementation Mechanisms

Interviews with the GES officials confirmed that there is no existing data protection policy. One interviewer said, "The GES body is responsible for developing policies for pre-tertiary schools for the management of data in schools; however, we do not have a data protection policy."

It was also found that none of the schools surveyed had a centralised digital records system. Instead, the data collected are normally kept on laptops and, in some cases, in hard copy formats in file cabinets. The mechanisms used to protect data are shown in Figure 5.

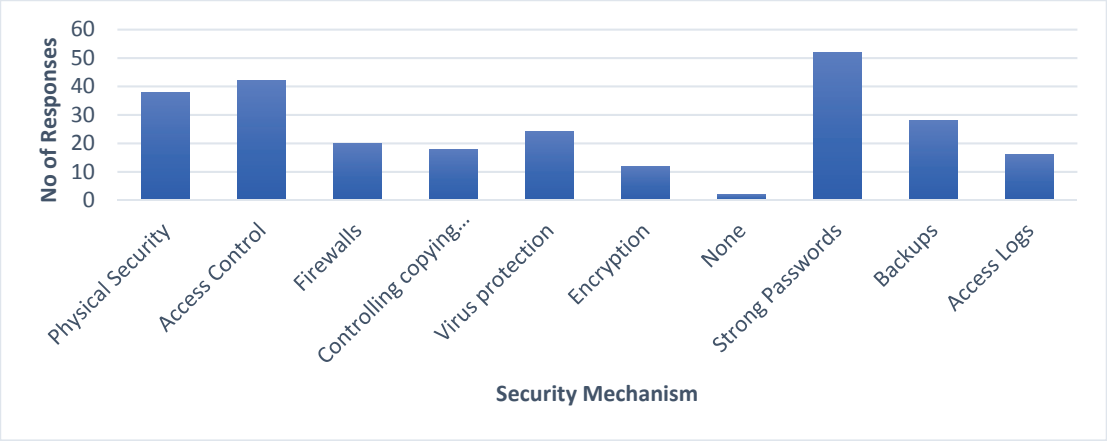

Figure 5: Mechanisms Used to Achieve Data Protection

Combining physical and digital storage across multiple schools, which are potentially unsecured locations, makes comprehensive data protection difficult. Additionally, the varied data protection mechanisms used by different schools imply a lack of standardised security protocols across schools, which can lead to security gaps. This situation could directly result from a lack of a data protection policy.

While these measures are essential for safeguarding data, they can still expose it to significant risks. For example, laptops can be lost or stolen, and sensitive data could be exposed if not properly encrypted or secured with strong passwords. Firewalls and virus protection help defend against external threats but do not address internal risks, such as unauthorised copying of data onto external drives. Though some schools indicated that they encrypted data on their laptops, it was clear that they did not encrypt data end-to-end when they were transferring data as they indicated that, in many cases, they transfer data using USB drives and instant messaging apps like WhatsApp. Such transfers subject the data to several risks as they could be easily shared.

7 Conclusions and Recommendations

Though most data managers know about Ghana's Data Protection law, a significant percentage do not understand the concept of data protection and do not know about their legal obligations. This is a serious challenge in achieving the goals of data protection.

Data protection in the pre-tertiary education system can be described as uncoordinated and fragmented and lacks formal guidance. It appears there is no coherent strategy to comply with the Data Protection law and/or achieve an acceptable level of data protection. As a result, the mechanisms deployed to achieve data protection also largely depend on the discretion of the staff designated to handle personal data. It was also found that the schools do not obtain explicit consent from data subjects, usually represented by their parents.

It is recommended that a comprehensive data protection policy or governance framework that standardises data protection practices across both physical and digital environments be developed based on a thorough risk analysis. As education institutions increasingly digitise and use electronic information systems, data protection training programs must be prioritised. Improving and institutionalising employee training and awareness will ensure that all staff understand the importance of data protection and the role they are supposed to play in maintaining it.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*, 509-514.

Berinato, S., & Perry, M. (2019). Security Trends by the Numbers. In *Insights You Need from Harvard Business Review*. Harvard Business Review Publishing Corporation.

Cahyaningrum, Y. (2024). Evaluation of System Access Security in The Implementation of MultiFactor Authentication (MFA) in Educational Institutions. *Journal of Practical Computer Science*, *4*(1), 11-19.

Chapple, M., Stewart, J. M., & Gibson, D. (2021). *CISSP: Certified Information Systems Security Professional Study Guide (9th Ed)* (3rd ed.). John Wiley and Sons Inc.

Cochran, W. G. (1977). *Sampling techniques* (3rd ed.). John Wiley & Sons Inc.

Creswell, J. W., & Clark, V. L. (2018). *Designing and Conducting Mixed Methods Research*. Sage publication.

Creswell, J. W., & Creswell, J. D. (2018). *Quantitative, Qualitative and Mixed Methods Approaches*. Sage publications.

Delgado-von-Eitzen, C., Anido-Rifón, L., & Fernández-Iglesias, M. J. (2024). Nfts for the issuance and validation of academic information that complies with the gdpr. *Applied Sciences*, *14*(2), 706.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 31-50 (1995).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Pub. L. No. L 119, 1–88 (2016).

European Union Agency for Cybersecurity. (2019). Handbook on security of personal data processing. In. Heraklion, Greece: European Union.

Ghana Education Service. (ND). *About Us*. Ghana Education Service.

Ghana Education Service Council. (2017). Code of Conduct for Staff of the Ghana Education Service. In G. E. Service (Ed.). Accra.

Limba, T., & Šidlauskas, A. (2020). Personal Data Processing in Educational Institutions: Anonymisation and Pseudonymisation. 13th annual International Conference of Education, Research and Innovation, Online.

National Institute of Standards and Technology (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). In. Gaithersburg, MD: U.S. Department of Commerce.

Pangrazio, L., Selwyn, N., Cumbo, B. J. J. L., Media, & Technology. (2022). A patchwork of platforms: mapping data infrastructures in schools. *48*, 65 - 80.

Data Protection Act, 2012 (Act 843), (2012).

Peng, Z., Liang, F., & Mu, L. (2022). Big Data□Based Access Control System in Educational Information Security Assurance. *Wireless Communications and Mobile Computing*, *2022*(1), 2853821.

Runtuwene, J. P., Mege, R. A., Palilingan, V. R., & Batmetan, J. R. (2019). Information security awareness on data privacy in higher education. 5th UPI International Conference on Technical and Vocational Education and Training (ICTVET 2018),

Samala, A. D., Mhlanga, D., Bojić, L., Howard, N.-J., & Pereira Coelho, D. (2024). Blockchain technology in education: Opportunities, challenges, and beyond. *International Journal of Interactive Mobile Technologies*, *18*(1), 20-42.

Schwartz, P. M., & Solove, D. J. (2011). The PII problem: Privacy and a new concept of personally identifiable information. . *New York University Law Review,*, *86*(6), 1814-1894.

Sinan, I., Tong, V. V. T., Nwoacha, V., Degila, J., Onashoga, A., Oaihimire, I. O., & Ukhurebor, K. E. (2024). Enhancing Security and Privacy in Educational Environments: A Secure Grade Distribution Scheme with Moodle Integration. *Journal of Infrastructure, Policy, and Development*, *8*(7), 3737.

Sirur, S., Nurse, J. R. C., & Webb, H. (2018). Are We There Yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR). 2nd International Workshop on Multimedia Privacy and Security, Toronto, Canada.

Smith, H. J., Dinev, T., & Xu, H. J. M. Q. (2011). Information Privacy Research: An Interdisciplinary Review. *35*, 989-1015.

van der Aalst, W. M. P. (2016). *Process Mining: Data Science in Action (2nd ed.)*. Springer.