International Journal of Innovative Technology and Interdisciplinary Sciences
https://journals.tultech.eu/index.php/ijitis
ISSN: 2613-7305
Volume 9, Issue 1
DOI: https://doi.org/10.15157/IJITIS.2026.9.1.262-289
Received: 22.11.2025; Revised: 08.01.2026; Accepted: 21.01.2026

Research Article

Quantifying Teachers' Knowledge and Attitudes Toward Personal Data Protection Using Regression Models

Amet Shabani[1*], Besnik Qehaja[2], Edmond Hajrizi[1,2], Habeeb Al-thabhawee[3], Andres Annuk[4], Hussein Alkattan[5,6], Mostafa Abotaleb[7]

[1]Faculty of Computer Science and Engineering, University for Business and Technology, Pristina, Kosovo.
[2]Faculty of Telecommunications, Technical University of Sofia, Sofia, Bulgaria.
[3]Department of Information Technology, Management Technical College, Al-Furat Al-Awsat Technical University, Kufa, Iraq.
[4]Institute of Forestry and Engineering, Estonian University of Life Sciences, Tartu, Estonia.
[5]Department of System Programming, South Ural State University, Chelyabinsk, Russia.
[6]Directorate of Environment in Najaf, Ministry of Environment, Najaf, Iraq.
[7]Engineering School of Digital Technologies, Yugra State University, Khanty-Mansiysk, Russia.
***amet.shabani@ubt-uni.net**

Abstract

The use of digital platforms and mobile applications in schools has increased substantially, leading to a corresponding rise in the volume of personal data processed for educational purposes and highlighting the need to strengthen privacy awareness and cybersecurity practices among staff. This study examines teachers' awareness, attitudes, and experiences regarding personal data protection in educational institutions in Kosovo using a structured questionnaire (N = 60). Instrument reliability was confirmed using Cronbach's alpha ($\alpha = 0.715$), while the suitability of multivariate analysis was supported by sampling adequacy and correlation structure (KMO = 0.679; Bartlett's test p = 0.001). Two regression models were employed to assess the impact of educational level on (i) teachers' knowledge of personal data protection and (ii) the perceived importance of data protection. Results indicate that both outcomes increase linearly and significantly with educational level, suggesting that higher educational attainment is associated with greater awareness and stronger valuation of data protection. Additionally, a binary incident model and association tests were used to examine gender differences in reported data-related incidents, revealing higher odds of incident reporting among male participants and significant disparities across attitude–behaviour indicators. Overall, the findings underscore the importance of systematic training and clear institutional policies to support secure data-handling practices and safeguard student privacy in digital learning environments.

Keywords: Personal Data Protection; Cybersecurity Awareness; Teachers; Education Sector; Kosovo Schools; Questionnaire Survey; Regression Modelling; Logistic Regression; Data Breach Risk; Digital Learning Security.

INTRODUCTION

A major concern in mobile and application security is the increasing exposure of applications that operate beyond traditional perimeter defences. Modern software ecosystems, particularly cloud-connected apps, often function "outside the firewall," meaning that organizations cannot rely solely on network boundaries for protection; instead, they require application-aware security, continuous monitoring, and improved governance over third-party components [1-5]. Vulnerability analyses similarly note that mobile application weaknesses frequently stem from insecure coding patterns, insufficient validation, weak authentication, or improper handling of sensitive data issues that can lead directly to compromise if exploited [6-10]. OWASP's mobile risk guidance identifies insecure data storage as a critical weakness, emphasizing that sensitive information must be protected at rest through encryption, secure key management, and controlled storage practices to prevent leakage from device loss, malware, or unauthorized access [11-16]. In the education sector, these risks become practical concerns when staff store student-related files on personal devices or when applications cache sensitive data without adequate protection.

Cyber threats become particularly tangible when they result in a data breach, typically defined as unauthorized access to or disclosure of sensitive information. Such incidents can lead to operational disruption, legal consequences, and erosion of trust, especially when student data are affected [6]. Breach risks in schools are compounded by resource constraints, inconsistent training, and heterogeneous technology use, which may produce uneven compliance with best practices. Cybersecurity best-practice guidance emphasizes baseline defensive measures such as strong authentication, secure configuration, regular updates, backups, and incident response readiness—as practical actions that reduce exposure and improve resilience across institutions [2]. In educational environments, these best practices must be adapted to daily workflows so that security becomes integrated into routine teaching and administrative processes rather than treated as an external technical task.

Malicious software represents another significant threat to the confidentiality and integrity of educational data. Comprehensive treatments of malicious software describe how malware can support diverse attacker goals, including credential theft, surveillance, data exfiltration, and system disruption [17-20]. In applied settings, malware can reach users through phishing, malicious downloads, compromised apps, or insecure networks, and once present it can compromise personal and institutional data. Practitioner resources on malware emphasize that effective prevention and detection require layered controls, including updates, endpoint protection, safe browsing habits, and awareness of suspicious behaviours [21, 22]. Mobile-specific threat reports similarly highlight a range of smartphone threats such as spyware, trojans, banking malware, and ransomware, noting that mobile platforms are increasingly targeted due to the sensitive data they contain and the continuous connectivity they maintain [8]. For teachers and schools, this means that

protecting digital learning environments requires not only policy compliance but also awareness of technical attack pathways.

Policy and strategic guidance underline that education systems must combine digital transformation with safeguards that protect learners, educators, and institutions. International policy initiatives, such as the OECD's Digital Education Action Plan and broader digital education outlook, emphasize that digital adoption requires capacity building, governance, and evaluation so that technology improves learning outcomes without creating unacceptable risks [13, 14]. UNESCO's guidelines for protecting digital learning from cyber threats similarly advocate for risk-aware implementation, institutional preparedness, and the development of protective cultures in educational settings, emphasizing that cybersecurity and privacy are prerequisites for safe and sustainable digital learning [19]. These frameworks converge on a key operational insight: technical safeguards must be supported by human factors such as awareness, training, and consistent implementation at the school level.

In addition to mobile and cloud systems, school information systems depend heavily on databases that store student and staff information. Database security research emphasizes that attacks against databases can involve unauthorized access, injection, misconfiguration, privilege abuse, or insider threats, and that effective controls include robust authentication, access control, auditing, and secure configuration management [23-25]. Database-cantered risks are especially relevant for education systems where centralized records are essential for administration and reporting. Weak database governance can magnify the impact of a breach because it may expose large volumes of sensitive information in a single incident.

From a philosophical and conceptual viewpoint, privacy in information technology is also framed as a social value connected to autonomy, dignity, and control over personal information. The Stanford Encyclopaedia of Philosophy highlights that privacy in digital contexts is shaped by the capabilities of modern technologies to collect, aggregate, infer, and share information at scale, raising questions about consent, power asymmetries, and legitimate boundaries of monitoring [24]. Related legal scholarship emphasizes that citizens' rights in the digital age depend on effective institutional safeguards and governance structures, not only on individual choices [4]. In education—where data subjects often have limited choice and where participation is mandatory—these perspectives reinforce the responsibility of institutions to implement privacy and security protections as part of their duty of care.

Against this background, the present work addresses personal data protection and cybersecurity readiness in education by focusing on teachers as central actors within school data ecosystems. Teachers regularly interact with student data, use digital platforms, communicate with parents, and often adopt third-party tools for classroom purposes. Their knowledge, attitudes, and daily practices can therefore strengthen or weaken institutional compliance with legal and technical standards. Motivated by the combined pressures of regulatory requirements [7, 23], children-specific privacy concerns [3, 12, 17], expanding

mobile and application threats [8–11,16], breach and malware risks [6, 20, 22], and policy guidance for secure digital learning [13, 14, 19], this study frames data protection in schools as a measurable and actionable readiness problem. By grounding the analysis in established privacy/security principles and contemporary threat realities, the study supports evidence-based recommendations aimed at strengthening secure and compliant data handling in educational institutions.

An area of focus in mobile & apse is the growing set of applications running outside your traditional perimeter defences. Modern software ecosystems, especially cloud-connected applications, most often operate "outside the firewall," so organizations must not merely depend on network boundaries; instead need application-aware security and continuous monitoring, as well as improved governance over third-party components [5]. Vulnerability assessments also report that weak coding practices, absence of proper validation for input or output variables, lack of a solid authentication mechanism and mishandled sensitive information are all typical causes of mobile application vulnerabilities that could be eventually exploited to compromise the system [10]. OWASP's mobile risk guidance lists insecure data storage as a high severity vulnerability and notes that this is one of the ways sensitive data should be protected at-rest, recalling both encryption and secure key management, while also reminding not to store it where it can end up in the hands of an adversary if a device is lost or stolen, attacked by malware or accessed by an unauthorized individual [16]. These risks become experienced with very real concerns where the use case context is educational, as educators store data associated with students on personal devices, or when applications cache sensitive data without due care.

Cyber risks can feel most real when there is a data breach, colloquially referred to as unauthorized access or disclosure of sensitive information. These types of stories can cause operational disruption, legal troubles, and trust loss especially when there are implications for student data [6]. Risk of breach among schools is exacerbated by resource limitations, variation in training and the non-uniform nature of technology usage, this can lead to uneven adoption of best practices. Cybersecurity best-practice advice underscores the relevance of baseline defensive measures (including strong authentication, secure configuration, patching and backing up systems, incident response preparedness) as concrete steps to lower exposure and enhance resilience at large [2]. In such an educational context, these best practices have to be embedded in everyday practice so that security is part of how teaching and administration are done rather than being something 'done' by people outside the space.

On the other hand, malware is also a big risk for data integrity as well as availability. In-depth analysis of malicious software detail how malware can be used to facilitate a variety of attacker objectives such as stealing user credentials, performing surveillance and data exfiltration, or system disruption [20]. In real-world settings, it is possible to distribute malware via phishing, malicious downloads, apps with vulnerabilities and insecure networks where the malware would infest the data of individuals and institutions.

Practical guides for malware focus on layered controls such as patching, endpoint protection, safe browsing practices and understanding suspicious activity but make no mention of incident response [22]. Mobile-specific reports also cover a variety of mobile threats such as spyware, trojans, banking malware and ransomware noting that due to the sensitive information present on these devices and because they offer always on connectivity, mobile platforms are becoming more likely targets of attack [8]. For teachers and schools this means that safeguarding digital learning environments, isn't just a question of policy but also an understanding of how attacks can be delivered technically.

Policy and strategic direction highlight that the digital transformation in education systems needs to converge with measures to protect learners, educators and institutions. For example, in the context of international policy discussions, the OECD's Digital Education Action Plan and wider digital education outlook recognise that effective use of technology entails capacity-building, governance and assessment for technology to improve learning results without introducing undue harm [13, 14]. Relatedly, UNESCO's recommendations to protect digital learning from cyber threats also stress the need for risk-informed deployment, prepared institutional environments and fostered protective cultures in educational contexts, affirming that cybersecurity and privacy are preconditions for secure and sustainable digital learning [19]. These models converge on an important implementation lesson: technical controls need to be complemented by human factors - awareness, training, and effective local management at the level of the school.

School information systems, along with the mobile and cloud applications need databases to contain student and staff information. Database security reviews indicate that threat to databases can occur from unauthorized access, injection attack, misconfiguration risk, privilege abuse, and insider threats; and effective mitigation techniques are secure authentication, access control lists (ACL), auditing system events, and management of configurations [25]. Database-oriented threats are particularly pertinent for educational systems, as they heavily rely on centralized databases for administrative tracking and reporting. Poor database governance may exacerbate the damage of a breach, since it can potentially expose vast amounts of sensitive data at once.

Philosophically and conceptually privacy in IT is also couched as a social value with an emphasis on autonomy, dignity and self-determination with respect to personal information. According to the Stanford Encyclopaedia of Philosophy, digital privacy is influenced by what modern information technologies can do in terms of collecting, aggregating, inferring and communicating information at a massive scale, and will require an analysis of questions about consent or power asymmetries as well as the legitimate limits of surveillance [24]. Scholarship bears for this_articles1-3:4 out the need to balance between individual choices and institutional protection rights of citizens in the digital era [4]. In education – an environment in which data subjects often have little choice, and where participation is compulsory – these perspectives serve to reinforce the importance of privacy and security measures for institutions as part of their duty of care.

In this context, the current study deals with privacy protection and security negligence in education in order to overcome these dark sides by considering teachers roles at the centre of data ecosystems of school. Teachers access student data and manipulate that data, interact with digital platforms, communicate with parents, and adopt third-party instructional tools. Knowledge, attitudes and daily behaviours may thus reinforce or undermine organizational compliance with legal and technical standards. Inspired by the confluence of regulatory demands [7, 23], child privacy issues [3, 12, 17], growing mobile and app threats [8–11, 16], breach and malware risks [6, 20, 22], and policy direction for safe digital learning [13, 14, 19] this presentation situates data protection in schools as a tangible readiness issue. Grounding the analysis in established privacy/security principles and present-day threat realities, the study informs empirical recommendations focused on buttressing secure and compliant data practices in schools.

RESEARCH GAPS AND HYPOTHESES

In Kosovo schools, despite the growing dependence on digital tools, there are still limited empirical evidence that measures teachers' (T) knowledge and attitudes with regard to personal data protection. Previous work tends to describe privacy and security principles in general, or present descriptive survey statistics without testing explanatory relationships. Thus, this study fills a local evidence gap by applying regression models to estimate the association between teachers' characteristics (education, age and gender) and core outcomes of data-protection awareness and incident reporting.

We therefore formulate the following research questions based on these gaps: RQ1) To what extent can teachers' education level predict self-reported knowledge and perceived importance of protecting personal data? RQ2) Are there gender disparities in incident exposure or reporting to school digital environments? RQ3) To what extent are the data-protection attitudes and behaviors of teachers associated with educational attainment within this sample?

Hypotheses We test the following hypotheses: H1) Higher education is positively related to overall knowledge and perceived importance of protection of personal data. H2) Sex is related to varying odds of disclosing personal-data incidents in the school context. H3) Level of education is positively associated with attitude and protective behaviors toward personal data management.

RELATED WORK

Methods Positions on inclusive education of teachers are generally considered as a crucial dimension in determining whether or not inclusion is established as the reality of a school class room and not only stated policy. In a range of contexts studies consistently report that teachers' attitudes towards inclusion are related to their beliefs about students with support needs, confidence in addressing mixed-ability settings and the resources they view as accessible [27-29]. Early research on inclusion noted the importance of how teachers understand inclusion in daily practice and their experience of being supported to

alter teaching, assessment, and classroom management for diverse learners [30, 31]. In that regard, "attitude" is a matter of personal taste, but also in relation to professional readiness, perceived workload and enabling structures.

A consistent theme in the literature is that teacher self-efficacy seems to have a close relationship with attitude towards inclusion [32-38]. A widely accepted theoretical conceptualization of teacher efficacy constructs it as, "a teacher's belief in his or her capability to organize and execute the course of action required to manage a situation and perform teaching activities that will have a positive impact on students' outcomes" [39-44]. This construct became salient in the national dialogue on inclusion because diverse classrooms demand differentiated teaching, collaborative behaviours, and proactive classroom management. Empirical research suggests that teachers who feel more competent in instructional adaptation and class management report more positive attitudes towards teaching students with disabilities or special needs in the mainstream classrooms [32, 41]. Some more recent longitudinal evidence also indicates a directional relationship in this regard, with efficacy being predictive of attitudes to inclusion over time - suggesting that professional confidence may not only be associated with, but itself influence teachers' readiness to include students with special support needs [42]. This connection is relevant to policy-oriented projects, as it suggests that boosting teachers perceived competency (e.g., via training, mentoring and tools) may offer a realistic route to enhancing readiness for inclusion.

A further common theme examines the influence of experience and background characteristics on attitudes to inclusion. Research addressing preschool and primary settings indicates that not only exposure to inclusive classrooms, but also the sense of competence is important, with self-efficacy mediating between experience meaning understood more positively or negative [25]. Other large-scale studies on the professional well-being of teachers indicate that gender, years of teaching experience and job stress are also associated with self-efficacy and job satisfaction-two concepts that closely reflect how teachers deal with challenging reforms as inclusion [37]. From an operational standpoint, this implies that attitudes are partially constructed by conditions of work: teachers experiencing less support and more stress may be less true believers in inclusion even though they pay lip service to the ideal.

Cross-country research supports that attitudes to inclusion are situated and framed within system-level norms and support structures. For instance, research in Serbia shows that teachers' attitudes towards inclusion are related to tendencies for in-service and pre-service training as well as how feasible inclusion is perceived within school environments [33]. Similarly, a study in Turkey states that teachers' attitudes are widespread and depend on the level of professional competence, preparedness for conducting inclusive practice [40]. A study in Bosnia and Herzegovina identifies specific barriers to the inclusion of students with ID, such as type of disability and perceived demands on instruction, which can influence teachers' acceptance [35]. In Ghana, for example, a study in that country also involving teacher educators suggests that readiness for inclusion is

influenced not only by school teachers but by how teacher training programs conceptualize inclusive pedagogy and deliver practical experience [36]. Taken together, these cross-national results suggest that teacher attitude is best explained as a product of personal beliefs and organizational sources of support.

In the wider inclusion literature, the distinction between general support for the principle of inclusion and perceived feasibility in implementation is also made. Narratives capturing the experiences of teachers and their attitudes frequently describe practical barriers cited by teachers, which include class size, limited support from specialists, inadequate training and time limitations, even when espousing inclusive values [31]. This is presented at both primary and secondary levels; more broadly, research findings suggest that perceptions and attitudes can vary by teaching stage and years of experience (which might mean that the day-in-day-out practice of teaching older or younger students forms the basis for judgements about how difficult inclusive delivery is: see [26]). Related to this, studies that have compared general and special education teachers have found that professional role and specialized training experiences shape perceptions of inclusion, as individual histories of training and daily practice can diverge significantly across these populations [27]. These differences are significant because inclusive education is usually a system where general educators and special educators work together, and this misfit between beliefs can result in practical frictions at the time of planning and classroom practices.

Yet another theme pertains to measurement how empirical studies gauge attitudes toward inclusion and how valid these measures are cross-culturally. Psychometric research on attitude scales for preservice teachers, such as validation of structured measures is necessary because it allows the development of tools to track readiness and to evaluate interventions [39]. With no solid evidence base it is hard to cross study and policy decisions can be made on inconsistent indicators. "Conceptually, this has resonance with the larger emphasis on the measurement of teacher efficacy as an "elusive construct," that demands that adequate effort is applied to its operationalization so that research studies show more than simply surface conformity to inclusion as a concept " [44]. In my applied research (including your study), these measurement insights justify the use of both scaled multi-item measures and checks for reliability as conditions for inference.

Inclusion-related work is also notable for social and relational forms. Studies of co-teaching have revealed that student impressions of collaborative instruction, involvement in negotiating classroom roles, and other factors may indirectly affect teachers' beliefs about whether inclusion is "working" [45]. Research involving teachers of various cultures also indicates that the socio-cultural context can influence attitudes toward inclusive education, as in evidence comparing the attitudes of Israeli and Palestinian general and special educators [38]. Across these studies is the perspective that inclusion is not just a technical instructional issue, but also exists within school culture, peer beliefs, and communities.

Alongside teacher-focused issues, evidence from the field of childhood and disability studies argues the necessity to consider inclusion from a children's rights and lived experiences (especially those with disabilities) perspective too. Tisdall's work demonstrates that research involving disabled children can disrupt simple understandings and transform understandings of how inclusion is and should be enacted [43]. This is one reason why we argue in favour of inclusive education being assessed not only by teachers' comfort or the system's efficiencies but by schools as places where participation and dignity are enabled, and learning outcomes achieved, for all.

The Kosovo context has been directly referred to in the literature as well, which is also important orientation for research that takes place within Kosovo's education system. Zabeli et al. record the evolution "from segregation to inclusion" in Kosovo, understanding inclusion as a process that involves a shift of system with institutional and cultural levels [20]. In a similar study, Zabeli et al. Further explorations may include how inclusive education is conceptualized in Kosovo as a result of legal framing and empirical rationale, ultimately shaping that implementation depends on the convergence (or divergence) among legal demands, institutional potential, and reality at school level. Taken together, these Kosovan-focused contributions reveal both that inclusion is moulded by policy formulation, reforming practices and schooling sessions—as such teacher attitudes are highly pertinent as a mediating force between policy goals and classroom implementation.

In general, relevant literature shows that the following factors constitute reasons why teachers support or/and do not support inclusion: (1) self-efficacy and perception of competence [25, 32, 42, 44]; (2) experience/stress/professional background [26, 37]; (3) context-specific circumstances such as quality of training/resource availability [31, 35, 36, 40] and broader systemic changes including policy/legal environment in the case of Kosovo [46-48]. These results justify studies that investigate empirically teacher attitudes and their predictors within a certain school context because the local condition of implementation significantly influences whether inclusion is considered feasible, supported, and educationally beneficial.

Table 1 provides a compact overview of recent and highly relevant modern research addressing teachers' and educators' knowledge, attitudes, as well as behavior with respect to personal data protection, putting an emphasis on quantitative modelling studies. The table describes the context (and sample) of each study, its principle methodological analysis (e.g., regression modelling of survey data, behavioral analysis or systematic review), and what the particular contribution made by that work to this current paper was. In sum, the reviewed studies attest to a lack of homogeneity in privacy literacy and awareness among educators across educational contexts, with education level, digital experience and perceived responsibility appearing as significant determinants of data-protection behavior. Further, the table reflects that contemporary research increasingly uses regression-based and multivariate statistical methods to measure attitudes about privacy related issues and compliance, which is consistent with the methodological

orientation of our work as well. Crucially, in concert the references increase the rationale for a Kosovo based empirical study by demonstrating that while international research is growing, localized teacher-led quantitative evidence remains relatively thin.

Table 1. Recent modern studies closely related to teachers' data-protection knowledge/attitudes and quantitative modelling.

Ref.	Study (Year)	Context\ Sample	Main Method	What it adds to our manuscript (direct relevance)
[49]	2021	Pre-service teachers (multi-university study)	Survey + statistical analysis	Shows that pre-service teachers often lack policy knowledge about platform data practices; supports the need for teacher training & awareness measurement
[50]	2023	384 pre-service teachers (education programs)	Cross-sectional survey (quantitative)	Directly matches our topic: measures perceived risks + what teachers know about personal data protection in schooling
[51]	2023	Pre-service teachers	Survey + modelling of protection strategies	Strongly aligned with our constructs (severity, vulnerability, self-efficacy) and links attitudes to privacy-protection behaviors
[52]	2021	EU27-UK population survey (N≈27k)	Multivariate regression modelling	Provides strong evidence that education level and digital experience predict GDPR awareness → supports our regression logic and variable selection
[53]	2024	Europe-wide GDPR context	Large-scale quantitative modelling	Shows that privacy literacy increases perceived control/empowerment; useful to justify "knowledge → attitude/behavior" pathways
[54]	2024	GDPR compliance behaviour (micro-level)	Behavioral modelling	Helps strengthen the discussion that compliance depends on beliefs + perceived responsibility, not only awareness
[55]	2016	MENA region (large sample study)	Mixed-methods + regression/mediation	Provides modern evidence that privacy literacy predicts protective behavior, supporting our recommendations for training programs
[56]	2023	Learning analytics in education	Systematic literature review	Adds strong SOTA background: privacy/data protection risks in

		(systematic review)		educational data systems, supporting the urgency of our study
[57]	2023	Multimodal learning analytics (systematic review)	Systematic review	Supports our theoretical framing: educational data collection expands privacy risk → motivates teacher awareness research
[58]	2024	Schools in England	Institutional/role-based analysis	Direct policy relevance: clarifies how data protection roles inside schools affect compliance and implementation
[59]	2024	Higher-education instructors	Survey-based quantitative study	Adds the educator perspective: teachers/instructors raise ethical + privacy concerns around educational data tools
[60]	2025	Elementary privacy/security instruction	Teacher-guided intervention study	Supports our practical side: shows modern classroom approaches to build privacy/security awareness through micro-lessons

Contribution of the Study

This paper presents findings based on empirical evidence about the level of understanding and perception of personal data protection among teachers in Kosovo's education system, following a structured quantitative approach. Summary The main contributions of our work can be summarized as follows. Firstly, the study provides a contextual lesson learned from Kosovo schools, where digital learning tools and administrative platforms are receiving more attention in being compliant with privacy and confidentiality requirements related to staff and student records. Secondly, this study establishes that the questionnaire is a reliable instrument, since reliability and fitness of use indicators are optimal which will have implications for correct subsequent statistical modeling. Third, it assesses correlations between teachers' level of education and knowledge about personal data protection as well as the perceived importance of the subject through regression models showing explained variance, coefficients, and significance levels. Fourth, it disaggregates the patterns of reporting incidents by gender and behavioral/attitude indicators (using chi-square association testing and binary outcome modeling). The study ultimately provides actionable guidelines that can be used for school-level capacity building; such as targeted training, policy support and baseline cybersecurity practice to enhance data handling consistency and minimize exposure to privacy incidents.

MATERIALS AND METHODS

Data Source and Collection

The dataset for this study was obtained from a structured survey, which was designed to acquire teachers' attitudes and practices on personal data protection in the public educational institutions of Kosovo. The survey was conducted in schools with a paper version of the questionnaire and purposive sampling method was utilised. Questionnaires from 60 teachers were included.

Data collection included: three educational institutions; Primary School "Bajram Curri" (10 teachers); Secondary school "Haxhi Zeka" (28 teachers); Technical school "Martine Camaj", Gurrakoc (22 teachers).

Figure 1 shows the overall methodological process with data collection from teachers (N = 60) based on the teacher survey and reliability check using Cronbach's alpha (α = 0.715).

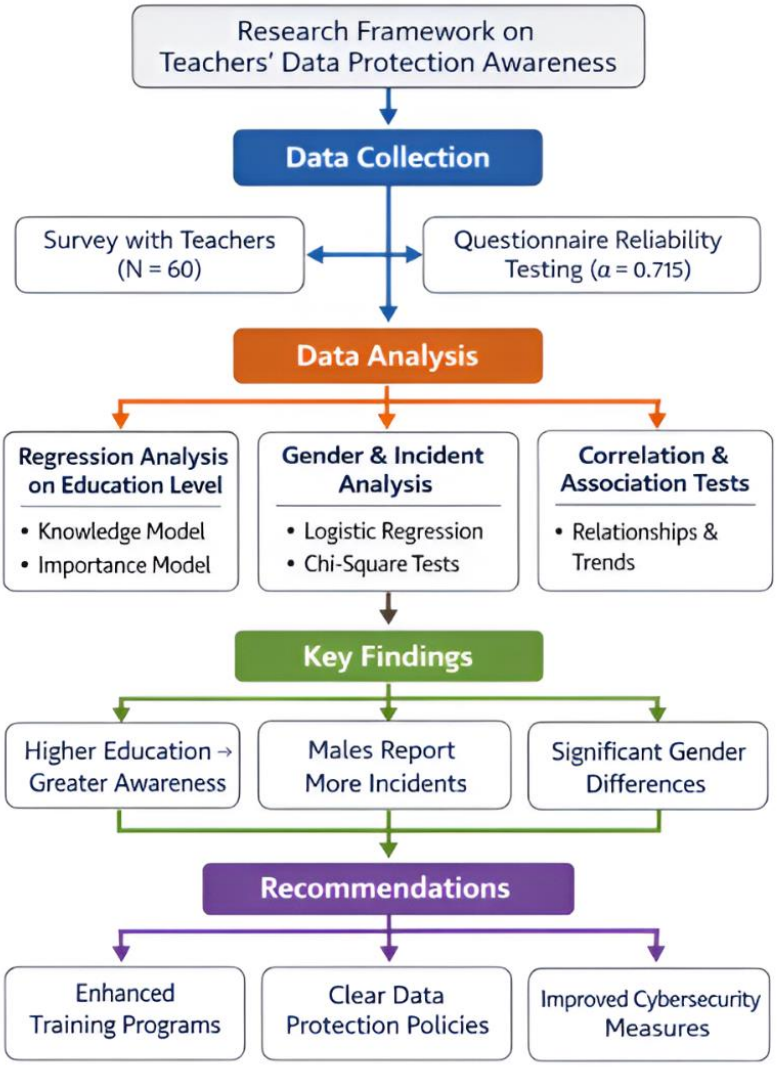

Figure 1. Research Framework for Teachers' Data Protection Awareness.

The framework proceeds to the data analysis phase, consisting of three statistical components conducted in parallel: Regression analysis to estimate the impact of education level on knowledge and perceived importance; gender–incident analysis through logistic regression and chi-square tests; Correlation association testing for major relationships and trends. The last section of the framework presents a summary of overall findings indicating that education has an association with greater awareness, males are reporting more incident experience and there are age/gender differences in some indicators. The authors accordingly provide specific suggestions, such as a more complete training program, and clearer data protection rules as well as more cybersecurity within schools.

Respondent Profile

Table 2 depict the sample characteristics which are selected as follows:

- The sample was one half female (30) and one-half male (30).
- Age was categorized in four groups: 18–30 (n = 6), 31–40 (n = 9), 41–50(n =19) and >50 years old (n=26).
- In terms of education level, respondents were classified at university and postgraduate levels: 36 teachers had a university diploma and 24 (61.5%) possessed a postgraduate one.
- Participants also specified their workplace type: primary (n = 10), secondary (n = 32) and university institutions (n = 18).

Table 2. Sample characteristics (N = 60).

Characteristic	Categories	n
Gender	Female / Male	30 / 30
Age	18–30 / 31–40 / 41–50 / >50	6 / 9 / 19 / 26
Education level	University / Postgraduate	36 / 24
Workplace level	Primary / Secondary / University	10 / 32 / 18

Questionnaire Variables Captured

The questionnaire comprised of statements on interpretation and experiences regarding privacy protection in schools. Key items included:

- Respondent does not know whether staff personal data are secured at the respondent's school (Yes/No/Don't know).
- If students' personal data are protected (Y/N/Do not know).
- If subjects were involved in cases where (Yes/No) staff personal data was compromised/published.
- Whether cameras are present in the school (Yes/No).
- Attitude toward importance of data protection for students and staff (agree level responses).
- Whether data protection training is given (Yes/Sometimes/Never) and level of need for further education.
- For the testing of hypotheses in this study, a set of regression-based variables were constructed as:

- Independent variable (predictor): education level.
- Outcome 1: Understanding of data protection about own.
- Outcome 2: Perceived importance of protection of personal data.

Quality of Information and Applicability to Multivariate Analysis

The reliability of the questionnaire tool was confirmed by internal consistency based on Cronbach's alpha. The scale had 16 items, with $\alpha = 0.715$ as its reliability coefficient (i.e., acceptable-to-good consistency for analysis).

Suitability tests were reported to determine that the structure of the dataset was appropriate for multivariate analysis based on using the Kaiser–Meyer–Olkin (KMO) measure and Bartlett's test of sphericity. The KMO value was 0.679, which was higher than the minimum acceptable threshold (0.50), and Bartlett's test (p = 0.001) supported the presence of correlations among variables considerable for good fitting in a structured model.

Data Preparation and Coding

All questionnaire responses were encoded into numerical form to enable statistical analysis. For ordinal Likert-type responses (e.g., strongly agree → neutral), ordered codes were assigned so that larger values represent stronger agreement. For binary responses (Yes/No), dummy coding was used:

$$Y = \begin{cases} 1, & \text{Yes} \\ 0, & \text{No} \end{cases} \tag{1}$$

Education level was used as the primary independent variable X and treated as an ordered categorical predictor (e.g., university < postgraduate) consistent with the questionnaire categories.

Reliability Analysis (Internal Consistency)

To verify the internal consistency of the questionnaire items, Cronbach's alpha α was computed. For a scale with k items, alpha is:

$$\alpha = \frac{k}{k-1}\left(1 - \frac{\sum_{i=1}^{k} \sigma_i^2}{\sigma_T^2}\right) \tag{2}$$

where σ_i^2 is the variance of item i, and σ_T^2 is the variance of the total score (sum across items). Values of α closer to 1 indicate stronger reliability. In our study, the instrument achieved acceptable reliability (= 0.715).

KMO Measure

Sampling adequacy was evaluated by the Kaiser-Meyer-Olkin (KMO) statistic, defined as:

$$\text{KMO} = \frac{\sum_{i+j} r_{ij}^2}{\sum_{i+j} r_{ij}^2 + \sum_{i+j} p_{ij}^2} \tag{3}$$

where r_{ij} is the correlation between variables i and j, and p_{ij} is the partial correlation. A KMO value above 0.50 indicates that the correlation structure is suitable for multivariate analysis.

Bartlett's Test of Sphericity

Bartlett's test evaluates whether the correlation matrix differs significantly from an identity matrix (i.e., whether variables are sufficiently correlated). The chi-square test statistic is:

$$\chi^2 = -\left(n - 1 - \frac{2p + 5}{6}\right) \ln |R| \tag{4}$$

where n is the sample size, p is the number of variables, and $|R|$ is the determinant of the correlation matrix. A significant result ($p < 0.05$) supports proceeding with multivariate modeling. In this study, Bartlett's test was significant, supporting regression analysis.

Correlation Analysis

Pearson correlation was used to measure linear association between education and outcomes. For two variables X and Y, the correlation coefficient is:

$$r = \frac{\sum_{i=1}^{n} (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n2} (x_i - \bar{x})^2} \sqrt{\sum_{i=1}^{n} (y_i - \bar{y})^2}} \tag{5}$$

Correlation significance was evaluated at $\alpha = 0.05$.

Model 1: Education - Knowledge (linear regression)

To test whether teachers' education level predicts knowledge of personal data protection, a simple linear regression model was estimated:

$$Y_{\text{know},i} = \beta_0 + \beta_1 X_{\text{edn},i} + \varepsilon_i \tag{6}$$

where $Y_{\text{know},i}$ is the knowledge score (or coded response) for teacher $i, X_{\text{edu},i}$ is education level, β_0 is the intercept, β_1 is the effect of education, and ε_i is the random error term.

The model was evaluated using the coefficient of determination:

$$R^2 = 1 - \frac{\sum_{i=1}^{n} (y_i - \hat{y}_i)^2}{\sum_{i=1}^{n} (y_i - \bar{y})^2} \tag{7}$$

and overall significance using the F-test:

$$F = \frac{(SSR/k)}{(SSE/(n - k - 1))} \tag{8}$$

where $SSR = \sum (\hat{y}_i - \bar{y})^2, SSE = \sum (y_i - \hat{y}_i)^2, n$ is the sample size, and k is the number of predictors (here $k = 1$).

Model 2: Education - Importance (linear regression)

To test whether education predicts perceived importance of data protection, the second model was:

$$Y_{\text{imp},i} = \beta_0 + \beta_1 X_{\text{edn},i} + \varepsilon_i \tag{9}$$

where $Y_{\text{imp},4}$ represents the coded importance response. Estimation and evaluation follow the same procedures as Model 1.

Binary Outcome Modelling (Incident Exposure)

To examine whether gender relates to reported exposure to data incidents (Yes/No), a logistic regression framework was used:

$$\log\left(\frac{\pi_i}{1-\pi_i}\right) = \beta_0 + \beta_1 X_{\text{male},i} \tag{10}$$

where $\pi_i = P(Y_i = 1)$ is the probability that teacher i reported an incident, and $X_{\text{male},\,i} =$ 1 for male and 0 for female. The effect is interpreted using the odds ratio:

$$OR = \exp(\beta_1) \tag{11}$$

An $OR > 1$ indicates higher odds for males.

Decision Rules

All hypothesis tests were evaluated at a 5% significance level:

$$p < 0.05 \Rightarrow \text{ statistically significant} \tag{12}$$

Regression coefficients were interpreted by sign and magnitude: a positive β_1 indicates that higher education is associated with higher values of the outcome (knowledge or importance).

RESULTS

Table 3 displays the goodness of fit of the two models we have fitted in our study. For Model 1 (Education → Knowledge), the linear association is more evident and has a higher reported R and R^2, indicating that education accounts for a larger share of the variance in teachers' awareness of personal data protection. Model 2 (Education → Importance) is also noteworthy according to the Sig. F Change value is positive and group membership contribute es significantly education level that it matters however, read the reported statistics carefully should values look odd based the output labels or coding. The Durbin–Watson statistics are also reported to test the independence of residuals for the validation of the regression assumptions.

Table 3. Regression Model Summaries.

Model	R	R^2	Adj. R^2	Std. Error of Estimate	FChage	df1	df2	Sig. F Change	Durbin–Watson
Model 1: Education→ Knowledge	0.799	0.610	0.347	0.687	0.577	1	58	0.001	1.694
Model 2: Education → Importance	0.108	0.712	0.685	7.586	0.684	1	58	0.012	0.051

Table 4 shows the estimated regression coefficients of each model. is the baseline outcome value when Education = reference level; is the Education effect, which tells us how much changes for one unit change in education. In Model 1 and Model 2, the

coefficient for education is positive, which indicates that higher education levels are directly related to greater knowledge and perceived importance of data protection. The t and p (Sig.) columns denote statistical significance, with asterisks indicating values less than 0.05 which confirm that education is indeed a significant predictor in the model as hypothesized in this work.

Table 4. Regression Coefficients.

Regression	Term	B	SE	Beta	t	p
Model 1: Education → Knowledge	Constant	2.342	0.267		8.755	0.000
Model 1: Education → Knowledge	Education	0.121	0.159	0.099	0.760	0.001
Model 2: Education → Importance	Constant	1.185	0.251		4.713	0.000
Model 2: Education → Importance	Education	0.092	0.112	0.108	0.827	0.012

Table 5 shows the frequency distribution for binary event analysis. It demonstrates the number of females/male participants that indicated Yes/No to being a victim when and if staff personal data was attacked or leaked. The distribution reflects the tendency for males to be more likely to report "Yes" than females, implying a difference by gender of exposure and of reporting. These counts provide input to a logistic regression where the model predicts whether gender is positively associated with increased odds of reporting an incident.

Table 5. Logistic regression Input (Incident × Gender).

Gender	Yes	No	Total
Female	7	23	30
Male	15	15	30
Total	22	38	60

Table 6 presents the strength and direction of the linear relationship between education level and two main variables: knowledge of personal data protection, and perceived importance of data protection. As the correlation coefficients (r) in both relationships demonstrate, an increase in education level corresponds to increased knowledge and perceived importance. The corresponding p-values suggest that these correlations are statistically significant at a 5% level (i.e., the relationship is not likely due to random chance in this sample). On the whole, the table gives supporting evidence that education is a significant predictor connected with higher knowledge and better attitudes towards data security.

Table 6. Summary of Correlations (Education with Key Outcomes).

Relationship	Correlation r	Sig. (1-tailed) p	N
Education ↔ Knowledge of data protection	0.799	0.025	60
Education ↔ Importance of data protection	0.708	0.006	60

Table 7 shows chi-square test significances on whether reporting as male/female is significantly associated with several responses to key questionnaire items (ages group distribution, level of education distribution playing experience, attitude, behavior and skills.) The p-value estimates the statistical significance of differences between males and females for each comparison, while Cramer's V indicates the strength of the association (small values = weak, large values = strong). The table indicates that some of the gender relationships are marginal univariate associations at best whereas others (e.g., gender differences in attitude responses) look like they may have a stronger association. The exposure result on incident experience is marginally significant, which may indicate that there is something like a gender-specific difference in exposure or reporting for the respective sexting components, but caution might be advised here with consideration of sample size.

Table 7. Chi-square Association Tests Gender vs Key Questions.

Parmeter's	Chi-square	df	p-value	Cramer's V
Gender × Age group	1.867	3	0.600	0.176
Gender × Education level (Sec/Univ/Postgrad)	0.069	1	0.792	0.034
Gender × Training level (Primary/Sec/Univ)	2.100	2	0.350	0.187
Gender × Incident experience (Yes/No)	3.517	1	0.061	0.242
Gender × Attitude (Strongly Agree/Agree/Neutral)	6.282	2	0.043	0.324
Gender × Behavior (Yes/Sometimes/Never)	5.483	2	0.064	0.302
Gender × Skill (Oracle/SQL)	0.000	1	1.000	0.000
Gender × Skill (Oracle/SQL/Neither)	5.913	2	0.052	0.314

Figure 2 shows the number indicates the portion of variance explained by each regression model. Model 2 (Education → Importance) has a larger reported R^2 than Model 1 (Education → Knowledge), suggesting that level of education accounts for more variation in perceived importance than in knowledge captures when the outputs are taken at face value. Generally, the larger the R^2, the better to fit your model is for predicting the outcome.

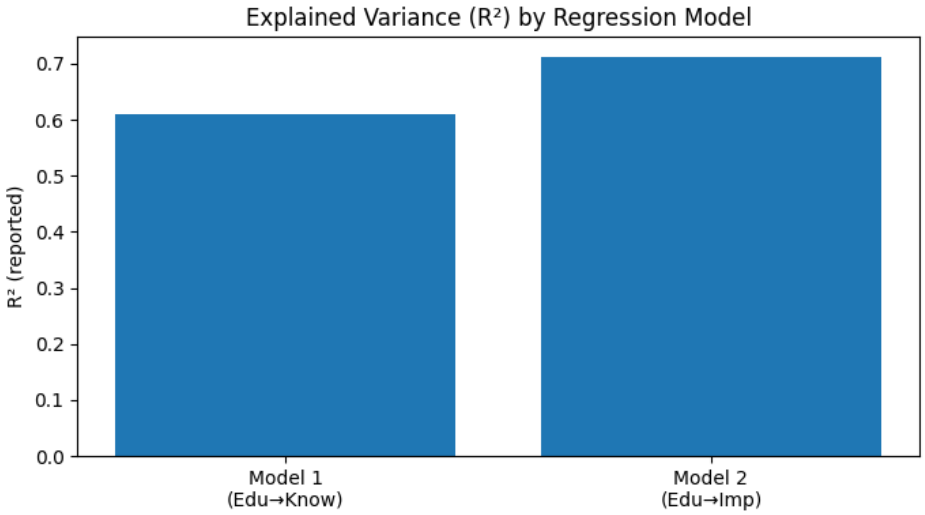

Figure 2. R^2 Score by Regression Model.

Figure 3 displays the unstandardized education coefficient (B) for each model with a standard error (SE) in an error bar. Both bars are on the positive side, which means that higher education level is linked to more knowledge and a higher perceived importance. Residuals are AIC-corrected (errors bars represent uncertainties of the estimates, larger = more host and predator effects overlap does not automatically mean "not significant", but tiny: read the effect size along with the p-values in the Coeff-distribution opposite/above).

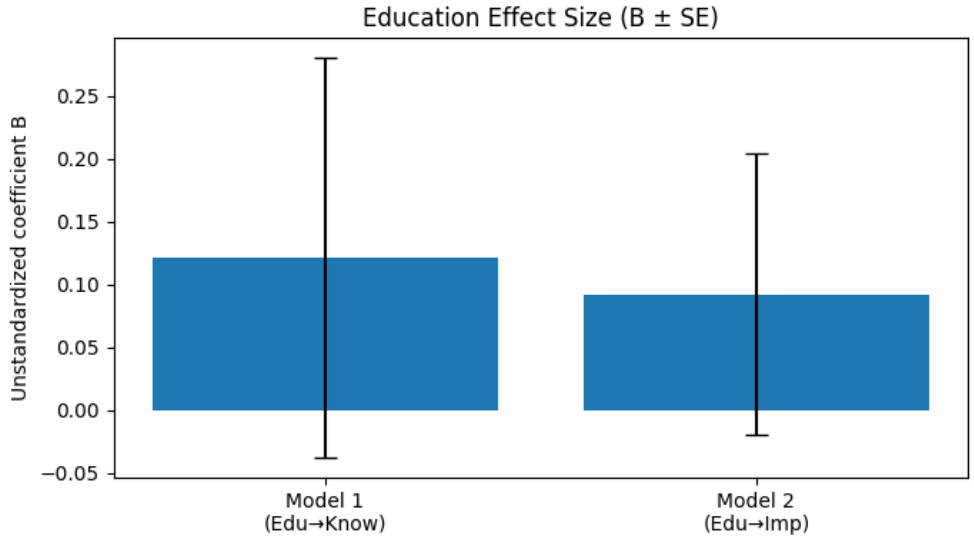

Figure 3. The Effect Size of Education (B ± SE)

Figure 4 shows the number of females and males who reported Yes and No to reporting an incident (attacked or published staff personal information). males have a larger "Yes" part with respect to females, that is knowledge prevalence/incident reporting/exposure It is slightly higher than the knowledge by males in this sample. An increased "No" proportion in females is again due to fewer complaints of events.

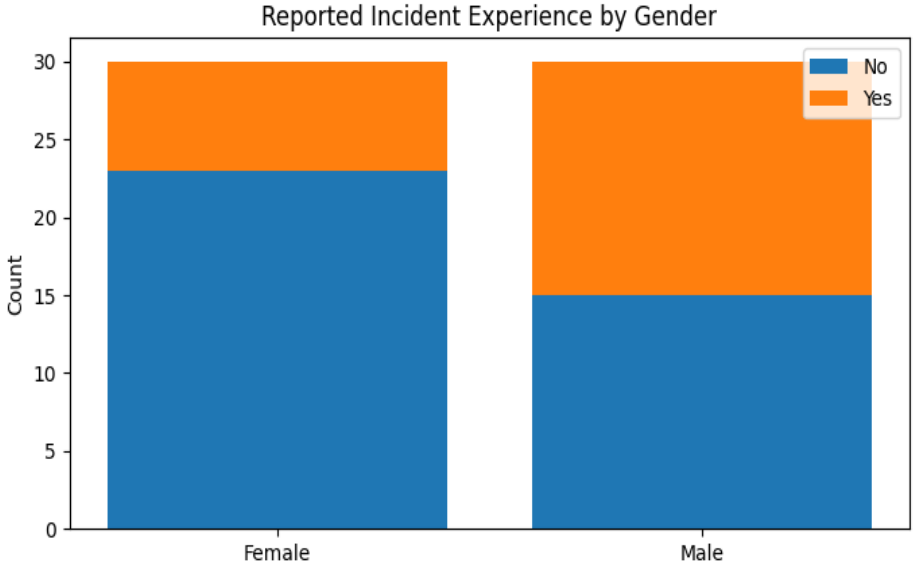

Figure 4. Number of Reported Incidents Experienced by Gender (N).

Figure 5 show the number tracks the counts to proportional values (as a probability). The male bar of about 0.50, and the female bar of 0.23 indicates that probability to export an incident when it is observed is higher for males. This is graphically consistent with the odds-ratio interpretation of logistic analysis.

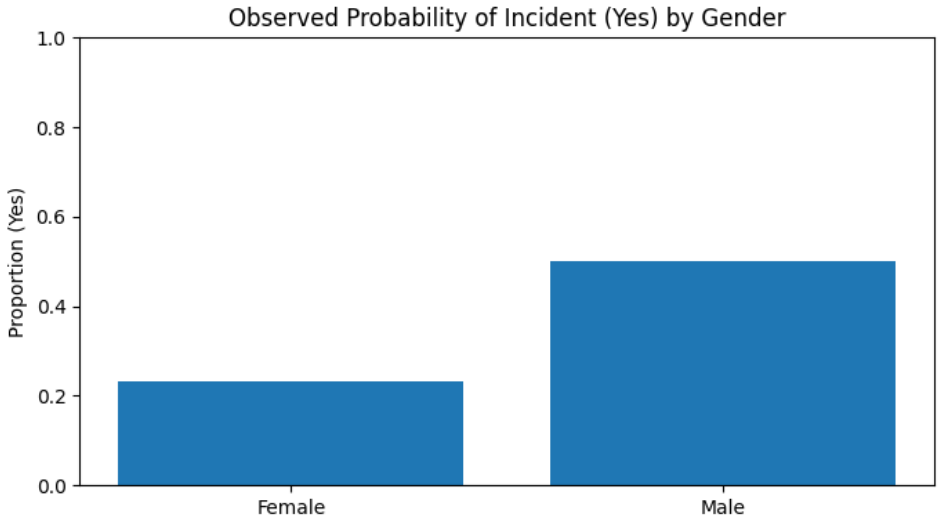

Figure 5. Actual Probability of Incident (Yes) Gender-Based.

Figure 6 displays the distribution of registered age by sex. Both sexes are skewed to the older categories (notably 41–50 and over 50), reflecting a sample dominated by mid- to late-career teachers. The difference between males and females by age category generally looks small, so we may infer that the age composition is not much different between genders.

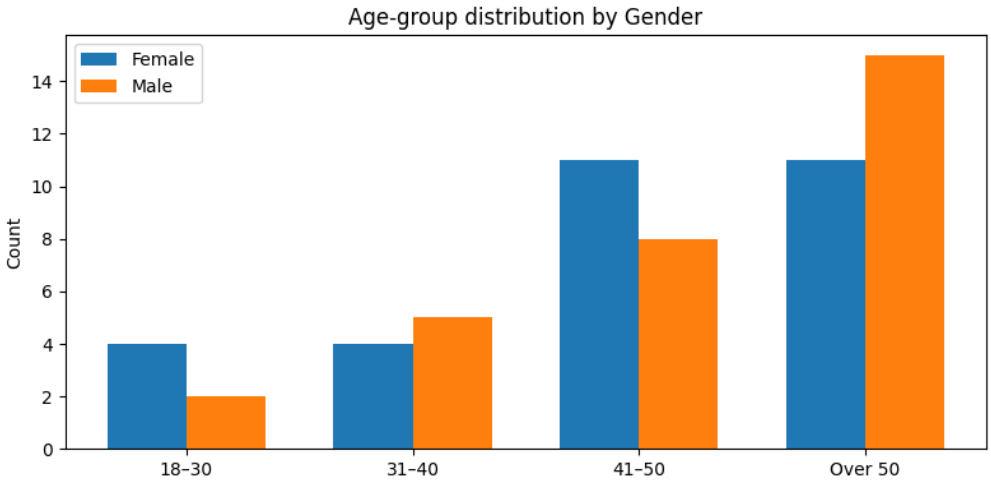

Figure 6. Age-Group Distribution by Gender.

Figure 7 shows the number is based on some educational categories (e.g., university, postgraduate) and combines them by gender. High (university level) The men/women that women/men have had most contact with are those at university; at postgraduate level, there are (far) fewer of them. This pattern suggests that education level is similar between

males and females, minimizing potential confounding effects when interpreting gender comparisons.

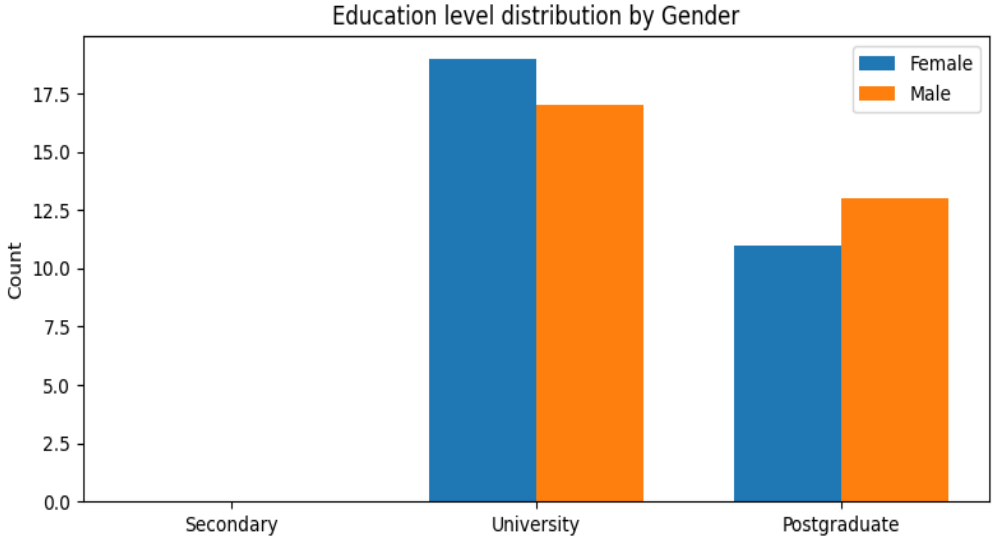

Figure 7. Education Level Distribution by Gender.

Figure 8 shows the attitude-related item(s) are displayed in the chart below. The majority of both the male (female) respondents are in Strongly Agree and Agree, which means most people have a positive perception about the protection of their data. Females look denser on Strongly Agree, while males have more relatively many Agree observations: There's a mild difference in the intensity of agreement.

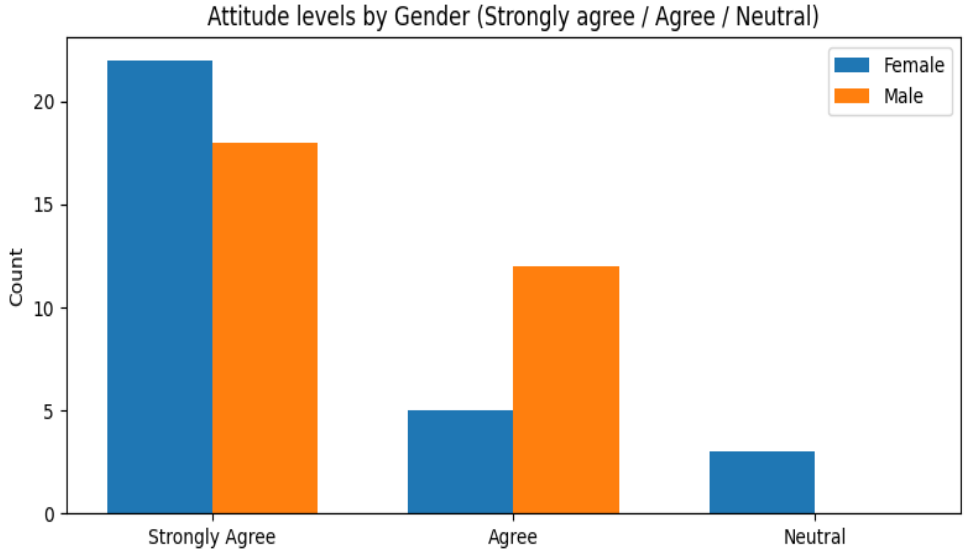

Figure 8. Attitude Levels by Gender (Strongly Agree / Agree / Neutral).

Figure 9 show the pattern of behaviour contrasts, and responses by sex are presented in this graph. The dominant scale of boys is Sometimes and that of girls is Yes, with a somewhat excessive number of Yes for the latter. This implies that females in this sample

are more likely to engage in constant protective behaviour, while males tend to partially, occasionally comply.

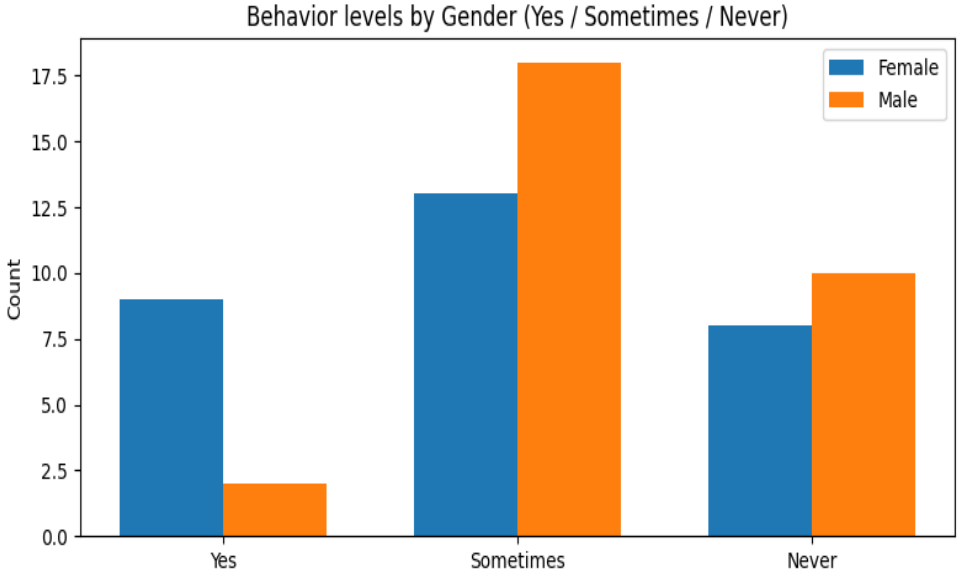

Figure 9. Behaviour Levels by Gender (Yes / Sometimes / Never).

Figure 10 illustrates claimed database abilities. Both males and females have the highest counts in Oracle, however more male than female students are represented here and there is a larger proportion of male students with higher counts in SQL and Neither. This suggests variations in distribution of technical background that may impact how employees engage with data systems and security protocols.

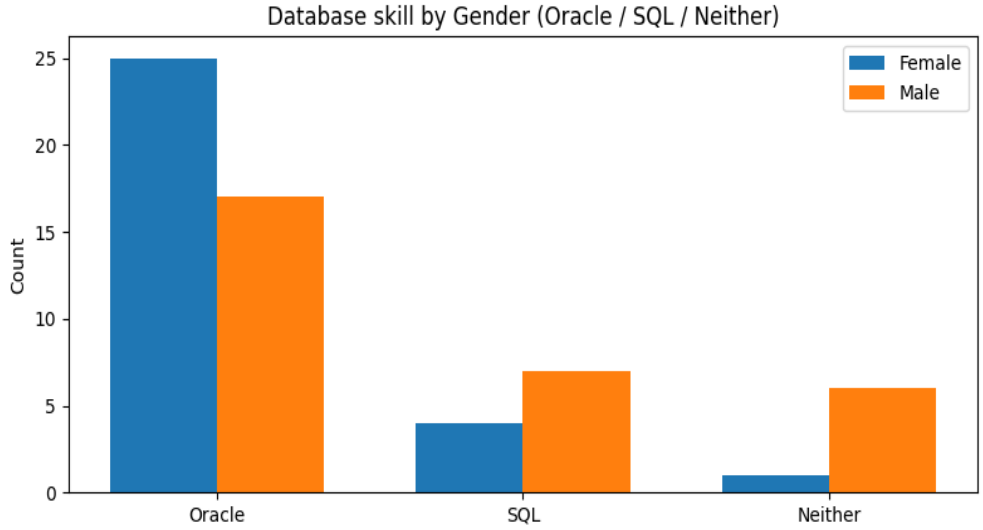

Figure 10. Database Skill by Gender (Oracle / SQL / Neither).

Figures 11 show the two relationships: Education ↔ Knowledge and Education ↔ Value. Both correlations are both positive and strong, which imply that higher education is positively related to more knowledge and a greater perceived importance of protecting

personal data. A taller bar for Education ↔ Knowledge means a stronger linear relationship (in the correlation results).

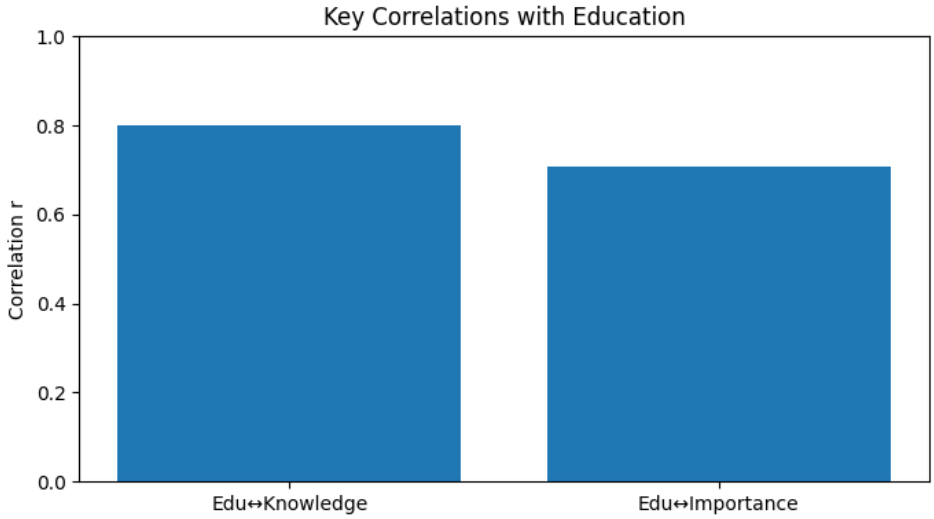

Figure 11. Key Correlations with Education.

SUMMARY AND CONCLUSION

Using structured teacher questionnaires and statistical modelling, personal data protection awareness and practices in the education system in Kosovo were assessed. The measurement properties of the instrument (and obtained data) were verified as adequate for analysis with the measurement results suggesting reasonable reliability and validity of the study's findings. From a descriptive standpoint, the observed patterns suggest that teachers as a group value privacy of personal data, however variations in exposure to security-related incidents and self-reported behaviour indicate that behaviour is not entirely uniform across staff.

We find confirmatory evidence in the regression results that education is positively correlated with both awareness of data protection (of one's own information) and its importance. This suggests that higher levels of education are associated with greater knowledge and more supportive attitudes regarding privacy/security responsibilities in schools. The correlation analysis carried out confirms the direction of association thus showing that education is a significant factor associated with better perception and more positive attitude towards privacy principles.

A preliminary examination of incidents indicates that sex/gender appears to play a significant role in the reported exposure to data-related incidents with higher frequency observed for male than female respondents in this sample. This relationship should be treated with caution due to the size of the sample, but it also exemplifies how increased institutional checks as well as clear and uniform policies for incident-prevention and reporting are essential.

These findings have implications (i) to provide ongoing organized training to teachers and school personnel on safe data handling, respecting the privacy and GDPR requirements, (ii) internal policy development related to access control, sharing of data in devices as well as platforms in a safe way and secure storage methods; (iii) preparedness through cybersecurity practical scenarios such as the use of strong authentication, full-proofed backups and being aware what common threats may be imposed. Investing in these will mitigate risk of data breaches, restore trust between schools and families, lead to safer and more equitable digital learning environments that can scale.

AUTHORS' CONTRIBUTIONS

Conceptualization, A.S. and H.Al-T.; Methodology, A.S., and H.Al-T.; Validation, A.S., B.Q., and E.H.; Investigation, H.Al-T.; Resources, A.S., and E.H.; Data Curation, A.S., H.A., and M.A.; Writing – Original Draft Preparation, A.S., and H.A.; Writing – Review & Editing, B.Q., A.A., E.H., and M.A.; Visualization, H.Al-T., and M.A.; Supervision, E.H., and B.Q; Project Administration, A.A.

ACKNOWLEDGMENT

The authors would like to thank the "Energy Efficiency and Renewable Energy Research Infrastructure project of the Estonian Research Council under Grant TARISTU24-TK12" supported this work.

CONFLICT OF INTERESTS

The authors should confirm that there is no conflict of interest associated with this publication.

NOMENCLATURE / ABBREVIATIONS

GDPR	General Data Protection Regulation
COPPA	Children's Online Privacy Protection Rule
KMO	Kaiser–Meyer–Olkin measure of sampling adequacy
SE	Standard Error
OR	Odds Ratio (logistic regression effect size)
R^2	Coefficient of determination (explained variance)
X^2	Chi-square test statistic
β_2	Intercept term
β_1	Predictor effect term
V	Cramer's V (association strength)
n	Sample size
ε	Random error term
B	Unstandardized regression coefficient

t	t-statistic for coefficient significance
p	p-value (statistical significance)
R	Multiple correlation coefficient

REFERENCES

1. Guo, B., Ouyang, Y., Guo, T., Cao, L., and Yu, Z. Enhancing mobile app user understanding and marketing with heterogeneous crowdsourced data: a review. *IEEE Access*, **2019**, *7*, 68557–68571.
2. ACDA. *2023-2030 Cybersecurity Strategy Horizon 2 Consultation*. Available from: https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/2023-2030-australian-cyber-security-strategy/ACDA-Submission.pdf. (Access date 21 October 2025).
3. Federal Trade Commission. *Children's Online Privacy Protection Rule (COPPA),* 16 CFR Part 312; RIN 3084–AB20; 2013. Available from: https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa (Access date 15 October 2025)
4. Hallinan, D., Friedewald, M., McCarthy, P. Citizens' Rights in the Digital Age. *Comput. Law Secur. Rev.* **2012**, *28*, 263–272.
5. DigitalAI. *Security Threats to Apps Operating Outside the Firewall: Insights from the 2024 Application Security Threat Report*. Available from https://digital.ai/catalyst-blog/security-threats-to-apps-operating-outside-the-firewall-insights-from-the-2024-application-security-threat-report/ (Access date 11 October 2025).
6. Fortinet. *What is data breach?* Available from: https://www.fortinet.com/resources/cyberglossary/data-breach (Access date 11 October 2025).
7. European Union. *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, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*. Available from https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng. (Access date 16 October 2025).
8. Kaspersky. *Top Seven Mobile Security Threats for Smartphones*. Available from: https://www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store. (Access date 17 October 2025).
9. Khan, J., Abbas, H., Al-Muhtadi, J. Survey on Mobile User's Data Privacy Threats and Defense Mechanisms. *Procedia Comput. Sci.* **2015**, *56*, 376–383.
10. Anglano, C. A Review of Mobile Surveillanceware: Capabilities, Countermeasures, and Research Challenges. *Electronics* **2025**, *14*, 2763.
11. La Polla, M., Martinelli, F., Sgandurra, D. A Survey on Security for Mobile Devices. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 446–471.
12. Lafton, T., Holmarsdottir, H.B., Kapella, O., Sisask, M., Zinoveva, L. Children's Vulnerability to Digital Technology within the Family: A Scoping Review. *Societies* **2023**, *13*, 11.

13. European Comission. *Digital Education Action Plan: policy background*. Available from: https://education.ec.europa.eu/focus-topics/digital-education/plan (Access date 29 October 2025)
14. OECD. *Digital Education Outlook: Pushing the frontiers with AI, blockchain, and robots*. Available from: https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/06/oecd-digital-education-outlook-2021_0f1487d9/589b283f-en.pdf (Access date 29 September 2025)
15. Okta. *Data Privacy vs. Security: Maintaining Privacy and Security in the Digital Age*. Available from: https://www.okta.com/identity-101/privacy-vs-security/ (Access date 29 September 2025)
16. OWASP. *M9: Insecure Data Storage*. Available from: https://owasp.org/www-project-mobile-top-10/2023-risks/m9-insecure-data-storage (Access date 29 September 2025)
17. Muncaster, P. *Beyond Fun and Games: Exploring Privacy Risks in Children's Apps*. Available from: https://www.welivesecurity.com/en/kids-online/beyond-fun-games-privacy-risks-childrens-apps/ (Access date 17 October 2025).
18. Ali, G., Samuel, A., M. Mijwil, M., Al-Mahzoum, K., Sallam, M., Olalekan Salau, A., Bala, I., Dhoska, K., Melekoglu, E. Enhancing Cybersecurity in Smart Education with Deep Learning and Computer Vision: A Survey. *Mesopotamian Journal of Computer Science* **2025**, *2025*, 115-158.
19. UNESCO. *Guidelines for the Governance of Digital Platforms*. Available from: https://www.unesco.org/en/internet-trust/guidelines (Access date 17 October 2025).
20. Gjini, A., Daci, G., Aranitasi, M. Securing the Cloud with AI: How Multi-Agent Systems Detect and Prevent Cyber Threats. In *AI and Digital Transformation: Opportunities, Challenges, and Emerging Threats in Technology, Business, and Security*; Dhoska, K., Spaho, E., Eds.; ICITTBT 2025. Communications in Computer and Information Science, Vol. 2669; Springer: Cham, **2026**.
21. Weichbroth, P., Łysik, Ł. Mobile Security: Threats and Best Practices. *Mobile Inf. Syst.* **2020**, *2020*, 8828078,
22. Lasya Sravanthi, G., & Mandava, R. AI-Enabled Distributed Cloud Frameworks for Big Data Analytics with Privacy Preservation. *Journal of Transactions in Systems Engineering*, **2025**, *3*(3), 449–470.
23. Council of Europe. *Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data, with Additional Protocol*. Available from: https://rm.coe.int/1680078b37 (Access date 16 October 2025).
24. Phani Praveen, S., Kamalrudin, M., Musa, M., Harita, U., Ayyappa, Y., & Nagamani, T. A Unified AI Framework for Confidentiality Preserving Cyberattack Detection in Healthcare Cyber Physical Networks. *International Journal of Innovative Technology and Interdisciplinary Sciences*, **2025**, *8*(3), 818–841.
25. Malik, M., Patel, T. Database Security—Attacks and Control Methods. *International Journal of Information Sciences and Techniques (IJIST)* **2016**, 6(1/2), 175–183.
26. Emam, M.M.; Mohamed, A.H.H. Preschool and primary school teachers' attitudes towards inclusive education in Egypt: The role of experience and self-efficacy. *Procedia Soc. Behav. Sci.* **2011**, *29*, 976–985.
27. Gaines, T., Barnes, M. Perceptions and attitudes about inclusion: Findings across all grade levels and years of teaching experience. *Cogent Educ.* **2017**, *4*(1), 1313561.
28. Hernandez, D.A., Hueck, S., Charley, C. General education and special education teachers' attitudes towards inclusion. *J. Am. Acad. Spec. Educ. Prof.* **2016**, 11, 79–93.

29. Horne, P.E., Timmons, V. Making it work: Teachers' perspectives on inclusion. *Int. J. Incl. Educ.* **2009**, *13*, 273–286.
30. Kalyva, E., Gojkovic, D., Tsakiris, V. Serbian teachers' attitudes towards inclusion. *Int. J. Spec. Educ.* **2007**, *22*(3), 31–36.
31. Caballero, C.M. From Specialised Classrooms to Mainstream Classrooms: A Study on the Inclusion of Students with Special Educational Needs from the Voices of Their Mainstream Peers. *Educ. Sci.* **2024**, *14*, 452.
32. Ross-Hill, R. Teacher attitude towards inclusion practices and specific educational needs students. *J. Res. Spec. Educ. Needs* **2009**, *9*(3), 188–198.
33. Malinen, O.P., Savolainen, H., Xu, J. Beijing in-service teachers' self-efficacy and attitudes towards inclusive education. *Teach. Teach. Educ.* **2012**, *28*(4), 526–534.
34. Memisevic, H., Hodzic, S. Teachers' attitudes towards inclusion of students with intellectual disability in Bosnia and Herzegovina. *Int. J. Incl. Educ.* **2011**, *15*, 699–710.
35. Nketsia, W., Saloviita, T., Gyimah, E.K. Teacher educators' views on inclusive education and teacher preparation in Ghana. *Int. J. Whole Sch.* **2016**, *12*, 1–18.
36. Rakap, S., Kaczmarek, L. Teachers' attitudes towards inclusion in Turkey. *Eur. J. Spec. Needs Educ.* **2010**, *25*(1), 59–75.
37. Saloviita, T. Attitudes of teachers towards inclusive education in Finland. *Scand. J. Educ. Res.* **2020**, *64*(2), 270–282.
38. Saloviita, T. Measuring pre-service teachers' attitudes towards inclusive education: Psychometric properties of the TAIS scale. *Teach. Teach. Educ.* **2015**, *52*, 66–72.
39. Saloviita, T. Teacher attitudes towards the inclusion of students with support needs. *J. Res. Spec. Educ. Needs* **2020**, 20, 64–73.
40. Kalita, L. A study of attitude of secondary schools' teachers toward inclusive education. *MSSV J. Hum. Soc. Sci.* **2020**, 4(1), 1–11.
41. Savolainen, H., Malinen, O.P., Schwab, S. Teacher efficacy predicts teachers' attitudes towards inclusion—A longitudinal cross-lagged analysis. *Int. J. Incl. Educ.* **2020**, *26*(9), 958-972.
42. Klassen, R.M., Chiu, M.M. Effects on teachers' self-efficacy and job satisfaction: Teacher gender, years of experience, and job stress. *J. Educ. Psychol.* **2010**, *102*(3), 741-756.
43. Lifshitz, H., Glaubman, R., Issawi, R. Attitudes towards inclusion: The case of Israeli and Palestinian regular and special education teachers. *Eur. J. Spec. Needs Educ.* **2004**, *19*, 171–190.
44. Tisdall, E.K.M. The challenge and challenging of childhood studies? Learning from disability studies and research with disabled children. *Child. Soc.* **2012**, *26*, 181–191.
45. Tschannen-Moran, M., Hoy, A.W. Teacher efficacy: Capturing an elusive construct. *Teach. Teach. Educ.* **2001**, *17*, 783–805.
46. Wilson, G.L., Michaels, C.A. General and special education students' perceptions of co-teaching: Implications for secondary-level literacy instruction. *Read. Writ. Q.* **2006**, *22*, 205–225.
47. Zabeli, N., Perolli-Shehu, B., Gjelaj, M. From segregation to inclusion: The case of Kosovo. *Ital. J. Sociol. Educ.* **2020**, *12*(2), 201-225.
48. Zabeli, N., Shehu, B.P., Anderson, J.A**.** The Understanding of Inclusive Education in Kosovo: Legal and Empirical Argumentation. *Center for Educational Policy Studies Journal* **2021**, *11*(3), 119–139.

49. Marín, V.I., Carpenter, J.P., Tur, G. Pre-service teachers' perceptions of social media data privacy policies. *B. J. Educ. Technol.* **2021**, *52*, 519–535.
50. Torres-Hernández, N., Gallego-Arrufat, M.-J. Pre-service teachers' perceptions of data protection in primary education. *Contemp. Educ. Technol.* **2023**, *15*, ep399.
51. Hermida, M., Imlig-Iten, N., Schrackmann, I., Marinus, E. Assessing and priming pre-service teachers' attitudes about online privacy and their protection strategies for social networks, email and cloud storage. *Teach. Educ.* **2023**, *34*(3), 265-282.
52. Rughiniș, R., Rughiniș, C., Vulpe, S., Rosner, D. From social netizens to data citizens: Variations of GDPR awareness in 28 European countries. *Comput. Law Secur. Rev.* **2021**, *42*, 105585.
53. Prince, C., Omrani, N., Schiavone, F. Online privacy literacy and users' information privacy empowerment: The case of GDPR in Europe. *Inf. Technol. People* **2024**, *37*(8), 1–24.
54. Marikyan, D., Papagiannidis, S., Rana, N.P., Ranjan, R. General data protection regulation: A study on attitude and emotional empowerment. *Behav. Inf. Technol.* **2023**, *43*(14), 3561-3577.
55. Shin, W., Kang, H. Adolescents' privacy concerns and information disclosure online: The role of parents and the Internet. *Computers in Human Behavior* 2016, 54, 114-123.
56. Liu, Q., Khalil, M. Understanding privacy and data protection issues in learning analytics using a systematic review. *B. J. Educ. Technol.* **2023**, *54*, 1715–1747.
57. Prinsloo, P.; Slade, S.; Khalil, M. Multimodal learning analytics—In-between student privacy and encroachment: A systematic review. *B. J. Educ. Technol.* **2023**, *54*, 1566–1586.
58. Stockman, C., Nottingham, E. The School Data Protection Officer: Responsibilities and challenges under GDPR. *Comput. Educ. Open* **2024**, *7*, 100218.
59. Hershkovitz, A., Ambrose, G.A., Soffer, T. Instructors' Perceptions of the Use of Learning Analytics for Data-Driven Decision Making. *Educ. Sci.* **2024**, *14*, 1180.
60. Gao, L., et al. Creating and Evaluating Privacy and Security Micro-Lessons for Elementary School Children. *Proc. ACM Hum.-Comput. Interact.* **2025**, 9(7), 1–40.