AJSIHD
GLOBAL RESEARCH NETWORK

AMERICAN Journal of Science on Integration and Human Development
Volume 3, Issue 5, 2025 ISSN (E): 2993-2750

Information Security and Personal Data Protection in Inclusive Distance Education

Isomaddinov Usmonali Mamurjonovich
Namangan State University, Lecturer at the Department of Information Technologies
uisomaddinov@gmail.com

Abstract: This article explores the multidimensional challenges and solutions associated with ensuring information security and protecting personal data within inclusive distance education environments. With the rapid expansion of digital education, inclusive platforms must handle sensitive information related to learners with disabilities, necessitating rigorous technological, legal, and ethical safeguards. This study analyzes global and national regulatory frameworks, including the GDPR [1] and Uzbekistan's data protection law [2], and evaluates the security infrastructure of prominent e-learning platforms (Moodle, Google Classroom, Microsoft Teams) [3]. Empirical data from educators and IT specialists are presented, revealing existing threats and gaps [4]. Based on comparative and technical analysis, the study offers practical recommendations for establishing resilient cyber security policies in inclusive digital education systems [5, 6].

Keywords: inclusive education, information security, personal data protection, GDPR, cyber security in e-learning, accessible digital platforms.

INTRODUCTION

The digital transformation of education has introduced new dynamics in pedagogy, particularly within inclusive learning environments. Inclusive education aims to provide equitable learning opportunities to all, including individuals with disabilities. With the adoption of distance learning modalities, an increasing volume of personal, medical, psychological, and educational data is being processed and stored on digital platforms. Such sensitive information, if exposed, may compromise learners' dignity, safety, and their right to privacy.

International data protection norms such as the European Union's General Data Protection Regulation (GDPR) [1] recognize disability-related information as a special category requiring enhanced protection. In parallel, Uzbekistan's national law "On Personal Data" [2] outlines rights and responsibilities concerning the collection, storage, and dissemination of personal information. However, the implementation of these regulations in educational institutions remains uneven, necessitating a thorough investigation.

This paper aims to critically analyze the state of information security and personal data protection in inclusive distance education, highlighting risks and proposing a framework for secure and ethical digital learning environments.

METHODS

This study employs a multi-method research design incorporating:

- Legal analysis: Review of GDPR (EU Regulation 2016/679) [1] and Uzbekistan's "On Personal Data" legislation (2020, updated 2023) [2] to understand the regulatory landscape.
- Platform audit: Evaluation of major distance learning platforms-Moodle, Google Classroom, and Microsoft Teams-focusing on their implementation of security features (SSL, 2FA, VPN, CAPTCHA) [3].
- Empirical survey: A structured questionnaire was administered to 73 university faculty and IT administrators across Tashkent, Andijan, and Namangan to assess knowledge, practices, and challenges [4].
- Comparative framework: International and domestic practices were compared to identify gaps and best practices in securing inclusive educational systems [5, 6].

RESULTS

Findings from the platform audits and empirical surveys revealed several security deficiencies in current practices. A detailed breakdown of technology implementation rates is provided in Table 1.

- Data encryption: 45% of surveyed institutions reported that learning management systems did not utilize encryption standards such as HTTPS or SSL [3].
- Authentication mechanisms: Only 30% had two-factor authentication (2FA) enabled [3].
- Unregulated data sharing: 64% of respondents admitted to sharing sensitive student information via unsecured channels (email, messaging apps). This discrepancy in security knowledge is clearly illustrated in Figure 1, which compares cyber security awareness levels between teachers and IT administrators [4].

Table 1. Implementation Rate of Key Security Technologies in Distance Education Platforms

Security Technology	Function	Adoption Rate (%)
SSL Certificates	Encrypt data in transmission	87%
2FA Authentication	Prevent unauthorized access	70%
VPN	Secure remote access	40%
CAPTCHA	Block automated threats	50%

Figure 1. User awareness of cybersecurity measures in distance education

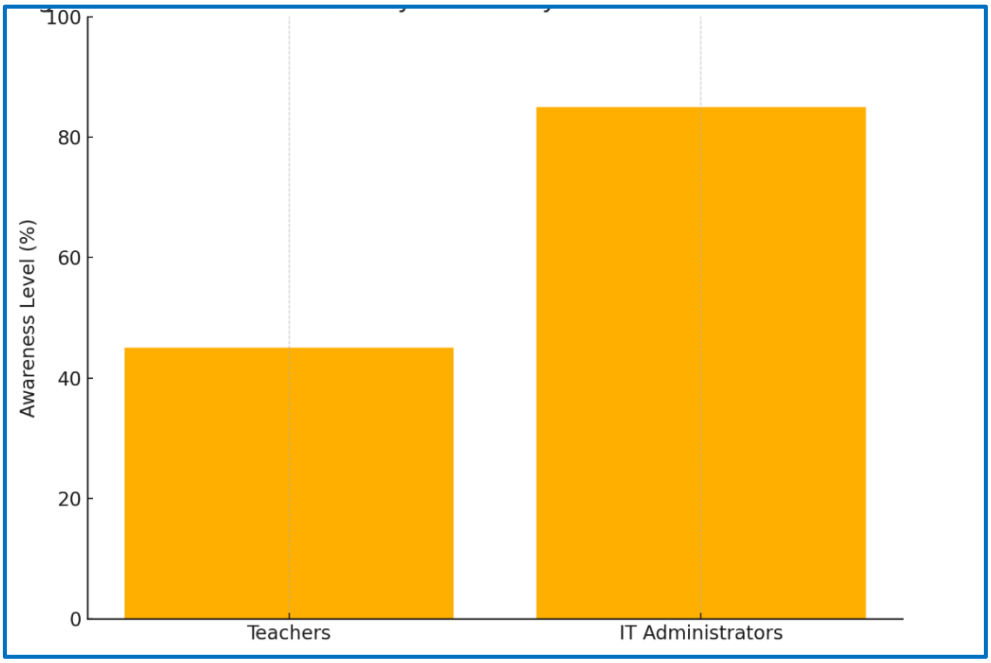
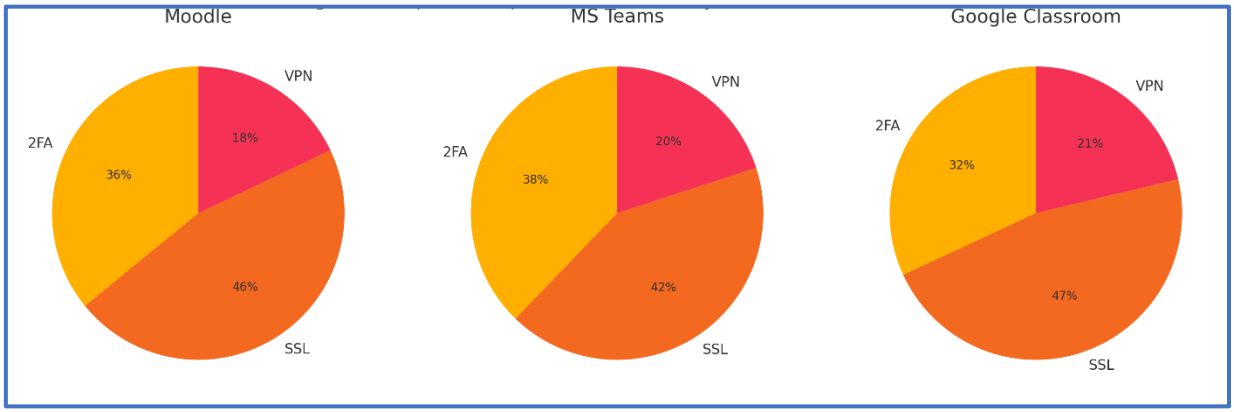


Figure 2. Comparative implementation of security features across platforms



DISCUSSION

The results confirm that inclusive distance education systems are vulnerable due to partial implementation of cyber security protocols and insufficient staff awareness. Figure 2 demonstrates this variation, highlighting the levels of 2FA, SSL, and VPN integration in Moodle, Microsoft Teams, and Google Classroom [3]. This creates a dual-layered risk: technological (due to software or hardware vulnerabilities) and human (due to negligence or lack of training).

International standards such as GDPR stress the principle of "privacy by design," advocating the integration of security measures at every layer of platform development [1]. In Uzbekistan, despite the adoption of national legislation [2], enforcement at the institutional level is fragmented, with many institutions lacking dedicated data protection officers [6].

Educators' limited knowledge about personal data handling further exacerbates the issue. Establishing a culture of digital responsibility, through mandatory cyber security training and user guidelines, is essential for creating a secure environment that respects the dignity and privacy of all learners, particularly those with disabilities [4, 5].

CONCLUSION

Information security in inclusive education must be approached not solely as a matter of digital infrastructure or software resilience, but as a core determinant of educational equity and the upholding of human rights. The integration of learners with disabilities into mainstream digital education systems introduces complex ethical and operational demands, particularly concerning the safeguarding of sensitive personal data. These include, but are not limited to, medical records, psychological assessments, individualized learning needs, and adaptive technology usage logs. As such, the integrity, confidentiality, and availability of this data are essential to maintaining trust in inclusive pedagogical models and to ensuring that the rights of vulnerable learners are preserved in virtual learning environments.

Drawing from empirical findings and comparative legal-technical analysis, this study proposes a set of strategic actions tailored to enhance the cybersecurity posture of inclusive educational systems:

1. Mandatory Implementation of Core Security Technologies (SSL, VPN, CAPTCHA, and 2FA): All learning management systems (LMSs) and digital education tools must incorporate standardized security protocols to safeguard data in transit and at rest [3].

- SSL (Secure Sockets Layer) ensures that all data exchanged between users and servers is encrypted.
- VPN (Virtual Private Network) restricts external tracking and unauthorized access to institutional networks.
- CAPTCHA mechanisms help prevent automated intrusions by malicious bots.

- 2FA (Two-Factor Authentication) adds a critical second layer of user identity verification, reducing the risk of account breaches.

2. Encryption and Tiered Access Control for Special-Category Data: Information relating to learners with disabilities is classified under the GDPR as "special-category personal data" [1]. Such data necessitates end-to-end encryption, role-based access control (RBAC), and logging of all access events [6]. Only authorized personnel-typically disability support coordinators, psychologists, or trained instructors-should have access to this information.

3. Capacity Building through Continuous Professional Development: Institutional cybersecurity cannot be achieved through technological intervention alone. Human factors remain the weakest link in most data protection systems. Thus, it is imperative to introduce mandatory periodic training programs on digital ethics, data classification, and safe data handling practices [4, 5].

4. Integration of GDPR Principles into National Cybersecurity Frameworks for Education: Educational institutions must act proactively to align their internal data protection policies with GDPR-aligned principles, such as:

- Lawfulness, fairness, and transparency
- Purpose limitation and data minimization
- Accuracy and accountability
- Integrity and confidentiality (security by design and by default) [1, 2]

5. Establishment of Monitoring, Auditing, and Incident Response Mechanisms: Cybersecurity must be seen as a dynamic process that evolves with threats. Institutions should form dedicated data protection units or designate Data Protection Officers (DPOs) responsible for the regular auditing of compliance, monitoring of vulnerabilities, and management of data breach incidents [6].

As digital education becomes increasingly prevalent, particularly in the wake of global health crises and accessibility-driven innovation, the safeguarding of learners' rights in cyberspace becomes a moral and operational imperative. Strengthening the digital foundations of inclusive education is not optional-it is essential to ensuring that no learner is excluded, exploited, or endangered due to systemic negligence in data protection. Only by embracing an integrated, rights-based approach to cyber security can educational institutions fulfill their commitment to equity, dignity, and inclusive excellence in the digital age.

REFERENCES

1. Voigt P., Von dem Bussche A., The EU General Data Protection Regulation (GDPR): A Practical Guide // Springer. 2017. https://doi.org/10.1007/978-3-319-57959-7
2. O'zbekiston Respublikasi, "Shaxsiy ma'lumotlar to'g'risida"gi Qonun, 2020-yil, №3РУ–632.
3. Liyanage L., Warnakulasooriya R., Comparative Study on Security Features in Online Learning Platforms // Int. J. Comput. Appl. Vol. 182. No. 5. 2019. P. 34–39. https://doi.org/10.5120/ijca2019918291
4. Bhardwaj K., Agrawal P., Tiwari S., Cybersecurity Awareness Among Teachers and Students in Online Education // Education and Information Technologies. Vol. 27. 2022. P. 11421–11440. https://doi.org/10.1007/s10639-022-11098-w
5. Chou C., Hsiao H.C., Internet Security: Malicious Software, Countermeasures, and User Awareness // Computers & Education. Vol. 48. No. 4. 2007. P. 460–478. https://doi.org/10.1016/j.compedu.2005.02.004
6. Raluca M., Protecting Personal Data in Digital Education: GDPR Implementation in Universities // Data Protection Journal. Vol. 3. No. 1. 2020. P. 14–27.