eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED INTERNATIONAL JOURNAL
Volume 05, Issue 05, May 2026

An Analytical Study of Cybersecurity and Data Privacy in Teacher Education

Mrs. Uttama Singh[1], Dr. Sabiha Anjum[1]
[1]B.Ed. (Education Training) Department, Dayanand Girls P.G. College, Civil lines, by CSJMU, kanpur

Received: 22 May 2026 Accepted & Reviewed: 25 May 2026, Published: 31 May 2026

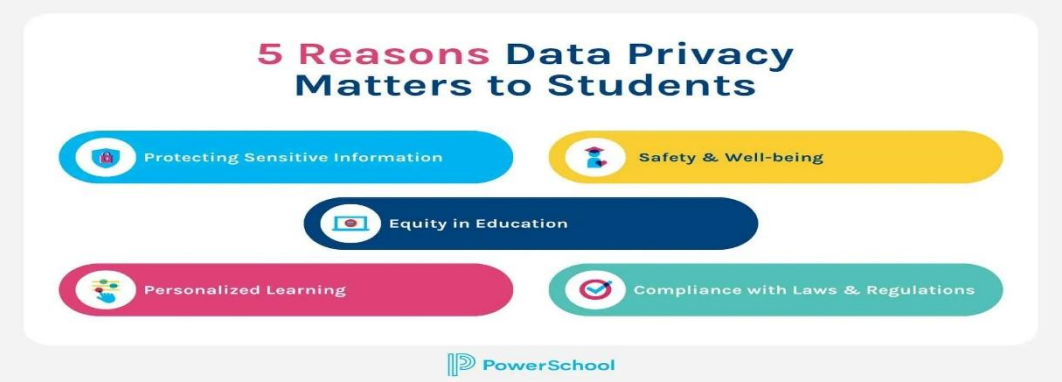
Abstract

The rapid integration of digital technologies into teacher education accelerated by national initiatives and the global drive to transform learning ecosystems has created immense opportunities and equally significant risks to cybersecurity and data privacy. This paper Qualitative analytical study and reviews literature on privacy and cybersecurity relevant to teacher education, study policy and regulatory contexts (international and Indian), articulates a theoretical way for analyzing privacy risks in teacher education . study to assess preparedness, practices, and perceptions among teacher educators and pre-service teachers. Digital transformation within teacher education has become central to national development initiatives, analytics-driven decision-making. These shifts have amplified risks concerning cybersecurity, data privacy, and ethical digital behavior. This research paper examines the theoretical, legal, and practical dimensions of cybersecurity and privacy within teacher education institutions (TEIs) with a national-level framework to support policy implementation, capacity building, and digital resilience across the teacher education ecosystem and practical policy recommendations, an institutional implementation and research implications for national transformation initiatives.

Keywords: cybersecurity, data privacy, teacher education, digital transformation, policy, India

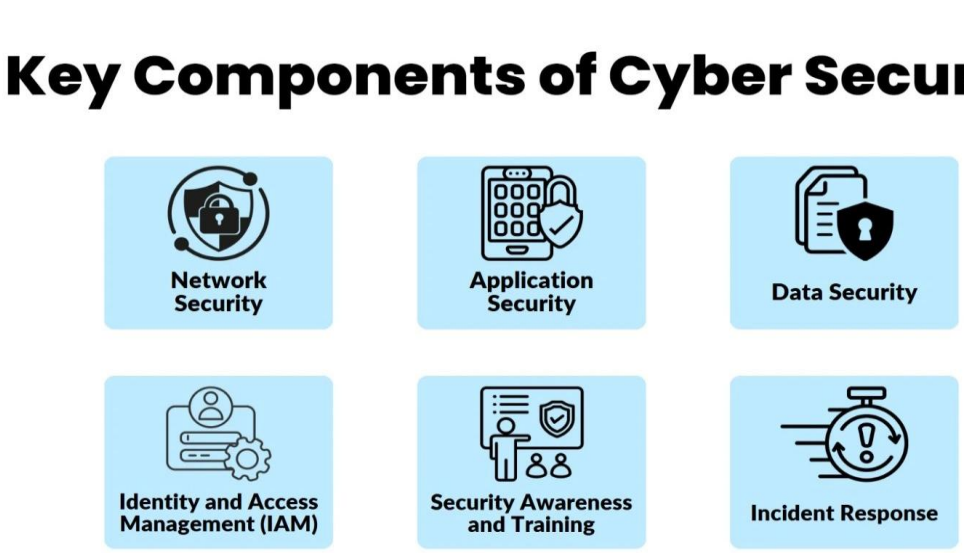
Introduction

Very Important role of Cyber security and data privacy in Teacher Education for Teacher educators and pupil Techers. Cybersecurity policies emphasize the need for secure cyber infrastructures. For teacher education, this means strengthening institutional governance, improving digital literacy, and preparing future teachers to safeguard educational data within their professional roles. The objective of cyber security education is to educate the users of technology on the potential risks they face when using internet communication tools, such as social media, chat, online gaming, email and instant messaging. Although there are many past research has been conducted on cyber security, in different areas less articles focused on the steps that need to be done particularly by schools in order to help cultivate cyber security awareness in detail. (Rahman,et al ,2020).While technology enhances pedagogical practice, access, and scalability, it simultaneously exposes teacher educators and pre-service teachers to cybersecurity threats and data privacy challenges. For nation-scale transformation in education to be sustainable, teacher education must embed robust cybersecurity and privacy-by-design practices.



eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED INTERNATIONAL JOURNAL
Volume 05, Issue 05, May 2026

Very Important role of Cyber security for Perspective Teachers it protecting school networks, student data, and personal devices from unauthorized access, cyberattacks, and data breaches. It requires practicing strong digital hygiene.



(Source :- Atul Kumar)

This paper explores the interplay between cybersecurity, data privacy, and teacher education within the broader aim of transforming the nation's educational capability. Technology Integration in Teacher Education. Educational technologies—LMSs, e-portfolios, AR/VR, analytics dashboards—are increasingly used in TEIs (Kumar & Nanda, 2022). Yet, teacher trainees often lack formal training in cyber hygiene, secure data handling, and ethical digital conduct (Punia & Kaur, 2021). Many Challenges in TEIs like a Absence of written institutional privacy policies Limited IT infrastructure and professional security staff .Over-reliance on third-party applications with Inadequate cyber hygiene practices (weak passwords, open Wi-Fi, device sharing) Poor documentation of incidents. TEIs must view cybersecurity and privacy not merely as technical issues but as ethical, pedagogical, and institutional responsibilities.

Strengthening these areas aligns with national digital transformation goals and prepares future teachers to navigate digital learning environments responsibly.

Objectives of the Study - To review existing literature, standards, and regulations relevant to cybersecurity and data privacy in education , assess knowledge, attitudes, and preparedness regarding cybersecurity and data privacy among teacher educators and pre-service teachers, map institutional policies, technical safeguards, and incident response practices in selected TEIs. the prevailing knowledge levels, perceptions, and practices concerning cybersecurity and data privacy among teacher educators and pre-service teachers and institutional policies, governance structures, and technical measures are in place in TEIs to protect educational data and gaps exist between policy and practice, and what contextual factors (resources, training, culture) influence these gaps

Literature Review- Privacy is commonly described as the right of individuals to control access to personal information and contextual norms governing information flows (Nissenbaum, 2004). Solove (2006) offers a taxonomy of privacy harms—information collection, processing, dissemination, and invasion—useful for analyzing educational data risks. Cybersecurity refers to the protection of systems, networks, and data from

theft, damage, or unauthorized access (NIST, 2018). Both domains overlap: strong cybersecurity supports privacy objectives, while privacy-aware policies constrain data handling and technical configurations. In educational contexts, privacy risks include unauthorized release of student performance and behavioural data, improper use of video or audio recordings from practicums, and harmful profiling from analytics. Cybersecurity threats include ransomware attacks on institutional servers, phishing targeting faculty, insecure third-party educational platforms, and misconfigured cloud services. Globally, frameworks such as the EU General Data Protection Regulation (GDPR, 2016) and international standards like ISO/IEC 27001 (information security management) and NIST Cybersecurity Framework provide legal and technical reference points. In India, national policies—National Education Policy (NEP 2020) and the Digital Personal Data Protection Act (2023)—frame obligations for institutions, while Ministries and regulatory bodies (e.g., UGC, NCTE) issue operational guidance. These policies emphasize data protection, consent, and institutional accountability, but implementation varies widely across TEIs. Studies on digital competence in teacher education emphasize the need to include digital citizenship, data literacy, and cyber hygiene in pre-service curricula. Embedding privacy-literacy and secure-technology pedagogy into teacher education prepares future teachers to model good practices in K–12 settings and to manage classroom technology responsibly. While literature examines student privacy in K–12 and higher education, targeted empirical work on teacher education institutions—particularly within India's policy context and transformation initiatives—is limited. There is a need for comprehensive studies that combine policy analysis, institutional audits, and stakeholder perceptions to produce actionable recommendations.

Conclusion

Achieving a nation-scale transformation in education requires that teacher education be digitally mature and privacy-protective. By integrating privacy literacy into curricula, strengthening institutional governance, adopting technical standards, and aligning procurement with legal obligations, TEIs can become trustworthy stewards of educational data. This paper provides a roadmap for research and practice to ensure that the digitalization of teacher education advances national goals without compromising cybersecurity or individual privacy.

Future Suggestion

Embed mandatory modules on data privacy, cybersecurity basics, and ethical technology use into pre-service programs. Include practical lab components (secure file-sharing, access control, safe online assessment design). Establish a Data Protection Officer (DPO) or equivalent in each TEI; create a cross-functional committee (academics, IT, legal, student representatives) to oversee data governance and vendor assessment. Adopt baseline technical controls: least-privilege access, multi-factor authentication, encrypted storage and transit, regular patching, backups with offline copies, and logging/monitoring. Use recognized standards (ISO/IEC 27001, NIST CSF) to structure controls. Require data protection impact assessments and negotiate data processing agreements that specify data residency, usage limits, deletion policies, and audit rights. Regular training (mandatory induction plus refreshers) for faculty, staff, and students. Scenario-based exercises to build resilience. Align TEI policies with national law (Digital Personal Data Protection Act, 2023) and international best practices; produce accessible privacy notices for learners and guardians. Government transformation initiatives should allocate dedicated funds and incentives for TEIs to upgrade cybersecurity, including grants for secure infrastructure and capacity development.

References-

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Digital Personal Data Protection Act, No. __, Acts of Parliament, (2023). Government of India.

ISO/IEC 27001:2013. *Information technology — Security techniques — Information security management systems — Requirements*. International Organization for Standardization.

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1). U.S. Department of Commerce.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119–158.

NPE/NEP. (2020). *National Education Policy 2020*. Ministry of Education, Government of India.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–564.