Digital Security & Media, 2(1),

16-31

Cyber Security in Primary and Secondary Education Institutions: A Document-Based Evaluation from Institutional, Teacher and Student Perspective

Received: 22/06/2025
Revised: 29/07/2025
Accepted: 31/07/2025

Murat Osman Kandır [1], **Serap Uğur** [2]

Abstract

This study investigates cybersecurity practices in Turkish primary and secondary education by analyzing official policy documents through a document analysis methodology. Without requiring ethical approval or field data collection, the study examines publicly available regulations and strategic plans from the Ministry of National Education (MoNE), the Information Technologies Authority (BTK), and the Personal Data Protection Authority (KVKK). Findings indicate that current Turkish policies emphasize technical security measures but lack sufficient structures for teacher training, student awareness, and institutional oversight. These policies are compared against the European Union's NIS2 Directive and the Cyber Resilience Act, revealing key discrepancies, especially in multi-factor authentication, incident logging, and staff training requirements. The study concludes that cybersecurity should be addressed not only as a technical issue but also as an educational and institutional priority, proposing a holistic vision for improving digital resilience in Türkiye's K-12 education system.

Keywords: cyber security, primary and secondary education, teacher competencies, student privacy, document analysis, digital security policies

Cite: Kandır, M., O.,,B, & Uğur, S. (2025). Cyber Security in Primary and Secondary Education Institutions: A Document-Based Evaluation from Institutional, Teacher and Student Perspective. *Digital Security & Media, 2*(1), 16-31

[1] Corresponding Author, 0000-0001-6918-6622, Eskişehir Osmangazi Üniversitesi, mkandir@yahoo.com
[2] , 0000-0002-4211-1396, Anadolu University, Faculty of Education, Türkiye, serapsisman@anadolu.edu.tr.

INTRODUCTION

With the penetration of digitalization into education, schools at the primary and secondary level are at the center of not only pedagogical transformation but also digital security threats. Devices connected to students' school networks, cloud-based tools used by teachers to produce digital content, and the integration of school administrations with e-government systems increase the need for a multi-layered cybersecurity architecture (ENISA, 2021; Zdrnja, 2024). Especially in the post- COVID-19 period, when distance education applications have become widespread, the vulnerability of educational environments to cyber threats has made it imperative to ensure the digital security of individuals as well as institutional risk management.

In Türkiye, the Ministry of National Education (MoNE) addresses cybersecurity from a technical

perspective in various strategic documents, focusing on topics such as information systems security, user authorization and data backup. However, implementation and monitoring mechanisms are limited in policy documents in areas such as teachers' cyber awareness in the context of digital literacy, students' ethical digital behaviors, and in-house log management (Tasay & Başaran-Demir, 2025; Yalçınkaya, 2023).

International literature reveals that cybersecurity education at the K-12 level is not systematically integrated into the curriculum; most practices are based on temporary projects (Ibrahim et al., 2024). The European Union made cybersecurity an obligation in 18 critical sectors, including education, with the NIS2 Directive published in 2022. This directive imposes concrete obligations on topics such as incident reporting, multi-factor authentication (MFA), mandatory in-house training and keeping log records (European Commission, 2023). The implementation guidelines published by ENISA point out that educational institutions should be equipped not only with technical competencies but also with human resources and awareness training (ENISA, 2025).

In this context, the cybersecurity policies of primary and secondary education institutions in Türkiye should be evaluated not only in terms of technical competence but also in terms of institutional obligations, teachers' professional roles and students' digital citizenship skills. However, it is seen that holistic evaluations that address these three actors together are limited in the literature. Most of the existing studies either focus on technical system security (e.g. server security, network protocols) or are limited to surveys that measure individual awareness levels.

The aim of this study is to examine cybersecurity practices at the primary and secondary level in Türkiye in the context of (1) institutional policies and legal obligations, (2) teacher training and awareness levels, and (3) students' digital security and ethical behavior skills. In addition, the current situation in Türkiye is compared with the European Union norms and current legal frameworks to identify policy alignment, strategic gaps and areas for improvement.

The study was conducted through document analysis of publicly available policy documents, and a methodology that does not require an ethics committee was adopted in the data collection process. The findings indicate that Türkiye needs to develop a multilevel strategy to create a sustainable cybersecurity vision in its digital education policies.

Problem Statement

Cybersecurity is a multidimensional area of digital resilience in education systems that is not limited to technical measures. Primary and secondary education institutions are responsible for both protecting students' personal data and developing their digital literacy skills. However, strategic documents and guidelines published by the Ministry of National Education (MoNE) in

Türkiye focus more on information systems security and the protection of information infrastructure, while the obligations related to the roles of teachers and students are not structured in a sufficiently systematic and traceable manner (MoNE, 2023; Yalçınkaya, 2023).

This situation leads to cybersecurity not being addressed as a pedagogical problem and thus neglecting the "human factor" in the education system. However, the European Union's NIS2 Directive of 2022 provides a comprehensive security framework that includes not only technical protection measures, but also mandatory training for all institutional employees, multi-factor authentication (MFA), logging, incident reporting and allocation of managerial responsibility (European Commission, 2023; ENISA, 2025).

In Türkiye, the current MoNE Information Security Directive defines the role of teachers only in terms of "user obligation", while for students it is often limited to general advice on ethical behavior or "responsible use of the internet". However, cybersecurity requires clear roles at the policy level, evaluation mechanisms, chain of control and curriculum-based education programs (Ibrahim et al., 2024; Tasay & Başaran-Demir, 2025).

In this context, the problem situation is embodied in the questions of to what extent the existing policy documents of primary and secondary education institutions in Türkiye on cybersecurity are adequate at three main levels (institution, teacher, student) and to what extent these structures are compatible with the European Union regulations. In this context, the main research questions of the study are as follows:

- What obligations do the cybersecurity policy documents implemented in primary and secondary education institutions in Türkiye include at the institutional, teacher and student levels?
- To what extent do the cyber security practices in these documents overlap with the European Union's NIS2 Directive and other EU regulations?
- What risks do the implementation gaps identified in existing documents pose for organizational sustainability and digital citizenship education?

LITERATURE

The integration of cybersecurity into the education system is possible not only through individual behavior change, but also through the multi-layered structuring of curricula, teacher training and institutional policies. In this context, firstly, approaches and teaching strategies related to cybersecurity in primary and secondary education should be examined on a global scale. Trends and practices in the international literature are instructive for assessing the current situation in Türkiye.

The integration of cybersecurity into the education system is not only limited to individual awareness and behavioral change; it is also possible through the multi-layered structuring of curricula, teacher education policies, governance mechanisms and institutional responsibilities. Especially at the primary and secondary education level, the strategic planning, execution and supervision responsibilities of the Ministry of National Education, provincial/district directorates, school administrations and IT coordinators for digital security are of critical importance. Within this institutional framework, pedagogical actors - especially teachers - need to be empowered with adequate equipment and support to effectively deliver digital security education in the classroom.

In this context, not only technical measures, but also governance decision structures, pedagogical strategies and institutional capacity stand out as decisive elements in building a cybersecurity culture. The following sub-section presents recent research findings on the global trends that feed this multi- layered structure and the current situation in Türkiye.

The following subsection presents current research findings on global trends.

Global Perspective: K-12 Cyber Security Education

Cybersecurity is no longer considered only as technical infrastructure security, but as a holistic learning area that is associated with individuals' capacity to develop conscious and safe behaviors in the digital environment. In this context, recent studies reveal that cybersecurity education at the K-12 level is still disorganized, unsystematic and not holistic enough on a global scale. A systematic review study conducted by Ibrahim et al. (2024), examining 24 scientific articles and 19 gray literature sources, found that cybersecurity education practices at the K-12 level are mostly concentrated at the secondary level; however, there is a serious lack at the primary level. The authors emphasized that integration at the curriculum level is mostly project-based and lacks sustainable learning objectives (Ibrahim et al., 2024).

The Scratch-based visual cryptography module, one of the applications developed to close this gap, was designed by Rayavaram et al. (2023) for secondary school students. This application, supported by interactive narrative scenarios, aimed to teach basic concepts such as confidentiality, integrity and authentication and achieved a learning success of 9.28/10 with 66.7% user satisfaction. This result shows that pedagogically based, age-appropriate and gamified content is effective in raising digital security awareness.

Teacher Perspective and Awareness

Teachers are the carriers and transformers of digital security culture in the educational environment. However, existing research shows that teachers' digital competencies are not sufficiently developed in terms of cybersecurity. Tasay and Basaran-Demir (2025), in their study conducted in the context of Türkiye, stated that teachers found students' digital awareness levels inadequate and stated that this situation was due to the lack of systematic cybersecurity education in teacher education programs. This finding suggests that in-service teacher training programs in Türkiye still do not include mandatory and assessed content on developing safe digital behaviors.

The systematic review conducted by Jayatilaka et al. (2021) emphasizes that cybersecurity awareness trainings should not be limited to the transfer of information; these trainings should be supported by interactive and practical content in a way to ensure behavioral change.

Corporate Responsibilities, Stakeholder Obligations and Implementation Guidelines

Effective implementation of cybersecurity in K-12 schools is not only limited to the individual awareness of teachers and students, but also requires clearly defined areas of responsibility,

governance mechanisms and monitoring and evaluation processes at the institutional level (OECD, 2021; ENISA, 2023). The digital security performance of educational institutions is a combination of strategic decisions taken at the top management level, the sustainability of the technical infrastructure and the interactive contribution of pedagogical actors (European Schoolnet, 2022).

The NIS2 Directive (2022/2555), which has been implemented in the European Union, envisages a multilevel responsibility matrix, including not only infrastructure providers but also public institutions and educational organizations. Within this matrix, school administrators are held responsible for the implementation of information security policies, teachers for student guidance, and IT staff for the prevention of systemic risks (ENISA, 2024). In addition, elements such as incident reporting, multi- factor authentication (MFA), log management and cyber security awareness trainings are mandatory for all employees (Zdrnja, 2024).

In Türkiye, although some circulars issued by the Ministry of National Education and the e-Safety Directive (2021) impose certain duties on school administrators and IT guidance counselors, these obligations are not comprehensive enough in terms of systematic supervision, performance measurement and legal binding (MoNE, 2021). For example, cybersecurity training for teachers is left at the recommendation level, while monitoring student behavior and intervention mechanisms are left to the school's initiative (Yalçınkaya, 2023).

Despite these gaps at the institutional level, local projects carried out by some private schools and metropolitan municipalities show that important steps have been taken towards teacher training and student awareness. However, these practices are generally unsustainable, based on individual initiatives and lack coordination (Güler & Ercan, 2022).

In this context, there is a need for a governance model that clearly defines the roles of all stakeholders (MoNE, school administrators, teachers, IT staff, parents and students), supports obligations with mutual control mechanisms and is applicable on a national scale. As stated in ENISA's 2023 "Cybersecurity Skills Framework for Education" document, defining cybersecurity roles, certifying technical competencies and ensuring the obligation of in-service training are the cornerstones of the institutional security infrastructure of the educational system.

When the current structure in Türkiye is compared with EU practices, it is seen that the well-intentioned orientations in the content of policy documents lack systematic integrity at the implementation level. Lack of coordination among stakeholders, ambiguity of job descriptions and discretionary awareness trainings constitute the weak links of corporate digital security.

Legal Framework at EU Level

The European Union treats cybersecurity not only as a technical imperative but also as a governance issue involving institutional capacity building and the human factor. The NIS2 Directive (Directive (EU) 2022/2555) imposes requirements on public service providers, including educational institutions, for authentication, security incident reporting, systematic logging and user awareness. Member states are required to revise their national regulations to comply with these standards by the end of 2024

(European Parliament & Council, 2024). Zdrnja (2024) states that this framework involves a paradigm shift that encompasses not only technical measures but also organizational structure, staff training and safety culture.

The implementation guide published by ENISA (2025) emphasizes that public organizations, including educational institutions, should clearly define their cybersecurity roles, build internal audit and crisis response capacity, and develop a systematic approach to ensure that all personnel receive a minimum level of training.

Theoretical Framework

The study is structured around digital public governance (OECD, 2018), the organizational cybersecurity maturity model (ENISA, 2021) and the individual digital competencies framework (DigCompEdu). In addition, the data responsibility framework of educational institutions in Türkiye is determined by the Law No. 6698 on the Protection of Personal Data (KVKK). In this context, it is emphasized that digital security in education does not only consist of hardware or software applications, but also the managerial structures, teachers' pedagogical responsibilities and students' digital citizenship skills should be evaluated as a whole (Yalçınkaya, 2023; Jayatilaka et al., 2021).

METHOD

This research is structured by document analysis method, which is one of the qualitative research approaches. Document analysis is a method that aims to examine the content of existing documents in a systematic, reproducible and theoretical context (Bowen, 2009). In this study, which did not require ethics committee approval, publicly available, legally binding documents and policy texts were analyzed. The research does not rely on empirical data collection; instead, it analyzes the implications of existing regulatory and directive texts for cybersecurity structures in the education system. In this context, the study adopted a model that combines institutional policy analysis and thematic content analysis methods (Merriam & Tisdell, 2016; Bowen, 2009).

Data Sources

Legal, administrative and strategic documents published by the Ministry of National Education (MoNE), Information and Communication Technologies Authority (ICTA) and Personal Data Protection Authority (KVKK) were used as data sources. The main documents reviewed are as follows:

- MoNE Information and System Security Directive (2016)
- Ministry of National Education Strategic Plan 2024-2028
- Regulation on National Education Directorates (2025)
- General Framework of Teacher Qualifications (2017)
- Teaching Profession Law (2023)
- Guidance Services Directive
- Regulation on Primary and Secondary Education Institutions
- Artificial Intelligence in Education Policy Document and Action Plan (2025-2029)
- ICTA Cyber Security Strategy Papers

Data Analysis Process

The data were analyzed using a thematic content analysis approach. The coding process was structured at the level of three actors (institution, teacher, student). Each document codified cyber security practices under the following headings:

- Access control and authentication
- Data security and KVKK compliance
- Level of education and awareness
- Monitoring, logging and auditing mechanisms
- Digital citizenship and ethical behavior

FINDINGS AND INTERPRETATION

In this section, institutional, teacher and student level policy documents on cybersecurity in primary and secondary education institutions in Türkiye are evaluated through thematic analysis. The findings are presented within the framework of themes coded at three levels.

Institutional Level Findings

The main document analyzed at the institutional level is the Ministry of National Education Information and System Security Directive (MoNE, 2016). This directive is MoNE's main document on protecting information assets, managing information security processes and

taking measures against cyber threats. The fact that it is dated 2016 shows that it comes from a period when the concept of cybersecurity was not yet so widespread, but that the ministry has paid attention to this area at an early stage.

The directive regulates password policies, user authorization, system access levels, content filtering and logging processes in detail. It also states that users' transaction logs on the network should be monitored, security breaches should be reported and measures should be taken against data loss. The Directive sets institutional standards for the security of information systems, access controls, backup, disaster recovery, security incident management, etc., covering all MoNE departments and affiliated institutions (and thus also primary and secondary education institutions). It indicates that school administrations should conduct risk analysis, establish security policies and implement technical measures for information systems and data. The security of school servers, network infrastructure and administrative databases is attempted to be secured under this directive.

However, the document does not include any provisions on the implementation of multi-factor authentication (MFA). There are also no clear statements on how logging systems are analyzed, how often audits are conducted and how audit outputs are reported. In addition, details on the structure and functioning of the SOME units envisaged to be established to respond to cyber incidents at the school level are insufficient.

The MoNE Strategic Plan 2024-2028 is a comprehensive document that sets out the Ministry's main goals, strategies and performance indicators for the next four years. Digitalization and the integration of information technologies into every stage of education is a key element of this plan, which increases the importance of cybersecurity. The Plan's objectives on the use of "Information and Communication Technologies" (ICT) and "Institutional Capacity Building" show that MoNE considers cybersecurity as an institutional priority. A secure digital infrastructure is a fundamental requirement for the uninterrupted and secure execution of all education processes. MoNE's Strategic Plan 2024-2028 sets out the Ministry's goals of improving the quality of education services, expanding their accessibility and raising individuals who meet the needs of the future. The plan strongly emphasizes digitalization, artificial intelligence, data management and the integration of information technologies into educational processes. This emphasis requires cyber security to be an integral part of the plan. The Plan makes important references to cybersecurity and data protection under the headings "Institutional Capacity" and "Quality in Education and Training".

The plan sets clear targets for improving institutional capacity and ensuring the security of information systems. MoNE Strategic Plan 2024-2028 positions cybersecurity as an important and integral component of the overall digital transformation and institutional capacity building goals of the education ecosystem. The plan addresses cybersecurity through both strengthening the technical infrastructure (institutional perspective) and improving the human factor (raising awareness and empowering teachers and students). In particular, the indicator "IT infrastructure and cybersecurity maturity level" is strong evidence that MoNE is taking a systematic approach to this issue. Successful implementation of this plan will significantly improve the cybersecurity resilience of primary and secondary education institutions in Türkiye.

However, the plan needs more specific and quantitative cybersecurity performance indicators such as reducing the number of cybersecurity breaches, shortening the response time to cyber incidents, and the rate of remediation of security vulnerabilities of critical systems. For example, targets such as the annual number of penetration tests, the frequency of vulnerability scans, and the rate of security patch implementation could have made the plan more concrete. There is no provision for clearly defining roles and responsibilities to ensure accountability in cyber security (such as a RACI matrix), or for establishing a cyber security management board or coordination unit. It would be useful to emphasize more explicitly the integration with the National Cyber Security Strategy and cooperation with USOM/SOME.

MoNE Strategic Plan 2024-2028 considers cybersecurity as a sine qua non of a modern institution and tries to integrate it into its strategic goals. However, as the plan remains at the "strategic" level, the objectives and activities in the area of cybersecurity still lack operational details. These gaps will often be addressed through lower-level action plans, directives and procedures. However, addressing these issues in a more concrete and measurable manner in the strategic plan will make the Ministry's commitment and roadmap on cybersecurity clearer.

ICTA's most recent and comprehensive strategy document is the National Cyber Security Strategy and Action Plan (2024-2028). Strategy documents have also been published for previous periods (2020- 2023, 2016-2019, 2013-2014). ICTA's strategy documents aim to increase the level of cyber security of all public institutions. MoNE is an important part of this overall framework. The ICTA's plan identifies ensuring the cybersecurity of critical infrastructures (such as energy, communications, banking, health) as a key priority. Education infrastructure (systems such as E-School, MEBBİS, EBA) is also considered critical in this context. MoNE has to increase the resilience of its central systems and the digital infrastructure in schools (networks, servers, end-user devices) against cyber-attacks. This requires compliance with the standards set by the ICTA (e.g. security controls, vulnerability management, penetration tests, security audits).

MoNE is expected to establish Cyber Incident Response Teams (CERTs) within its own organization (or in each school) or increase the effectiveness of existing CERTs. Cyber incident notifications should be integrated into ICTA's USOM system and MoNE should actively participate in national cyber security drills. The creation of "incident response plans" at the school level is also encouraged. MoNE must ensure that sensitive data belonging to students, teachers and administrative staff is protected to the maximum extent in line with the PDPL and national data protection policies. This includes

implementing data classification, encryption, authorization-based access and data leakage prevention (DLP) solutions.

The ICTA National Cyber Security Strategy and Action Plan is a high-level document that succeeds in setting out Türkiye's cyber security vision and core principles. However, due to the nature of such national strategies, they often lack operational details or enforcing implementation mechanisms on how the overall objectives will be materialized by individual public institutions. These gaps are often

addressed through lower level regulations, communiqués, guidelines or national programs. However, more references to such details in the strategy itself would contribute to making the implementation more effective and standardized.

Teacher Level Findings

The Regulation on Directorates of National Education (2025) aims to establish a consistent security infrastructure in schools by introducing centralized control mechanisms and standard protocols on cybersecurity. The most positive aspect for teachers is the clear definition of network security, data protection and emergency response procedures, thus giving the administration the power to sanction cybersecurity measures. In addition, improving teachers' digital literacy skills through regular cybersecurity trainings has also been a prominent regulation. However, there are ambiguities in the regulation in practical applications. Critical issues such as the process for teachers to report cybersecurity breaches, risk assessment methodology and budget for technical infrastructure are not clearly specified. Moreover, the lack of preventive measures, such as a digital security pledge from students and parents, increases the risk of schools being vulnerable to cyber threats. The most important gap is the absence of psychological support mechanisms for students who experience cyber victimization.

It was observed that the documents related to teachers, especially the General Framework for Teacher Competencies (MoNE, 2017) and the Turkish adapted versions of the UNESCO ICT-CFT framework, include digital security. In these documents, it is emphasized that teachers should use information and communication technologies safely for pedagogical purposes, select digital resources in line with ethical principles and pay attention to the privacy of student data (UNESCO, 2011).

The General Framework of Teacher Qualifications (2017) defines teachers' technology use competencies and digital literacy skills as part of professional development in line with the requirements of the digital age. The most important plus in terms of cybersecurity is that teachers' awareness of "digital security and ethics" is identified as a competency area. In this way, teachers are expected to guide students on issues such as password security, personal data protection and cyberbullying. Moreover, emphasizing skills for the safe use of the Education Information Network (EBA) and other digital platforms encourages teachers to use digital tools more consciously.

However, the framework document does not include concrete implementation steps and emergency procedures for cybersecurity. There is no clear guidance on how to act in situations that teachers may face, such as data breaches, ransomware attacks or cyberbullying. Furthermore, cybersecurity trainings are not integrated into continuous professional development programs, making it difficult for teachers to keep their knowledge and skills up to date in this area. The most important shortcoming is that the boundaries of teachers' responsibilities for cybersecurity (e.g. the extent to which they are responsible for the security of the school network) are not clearly defined.

The Law on Teaching Profession (2023) clearly defines the digital responsibilities of teachers, taking into account the implications of digital transformation in education. The most important plus of the law is that it obliges teachers to "comply with professional ethics in digital environments" and "protect the confidentiality of student data". In particular, the emphasis on the protection of personal data (KVKK) and respect for copyrights forms the legal basis for cybersecurity awareness. Moreover, the law's obligation to update teachers' digital skills as part of continuous professional development paves the way for cybersecurity trainings.

However, the law does not clearly define the limits of teachers' legal liability for cybersecurity breaches. For example, it is not clear to what extent a teacher will be held liable in the event of a data leak. Other important shortcomings include the absence of anti-cyberbullying protocols and emergency response mechanisms. Furthermore, there are no criteria for the security standards of digital tools to be used by teachers.

The 2017 Guidance Services Directive (2017), published in the Official Gazette in 2017, supports students' psychosocial development while addressing important contemporary issues such as cyberbullying and digital addiction. The most powerful aspect of the directive is that it places the responsibility on guidance counselors to provide digital citizenship trainings for students. In particular, the emphasis on "communication skills in the virtual environment" and "safe internet use" contributes to raising cyber security awareness. In addition, stating that psychological support mechanisms should be activated in cases of cyberbullying encountered by students is seen as a positive approach.

However, the directive does not adequately cover the technical aspects of cybersecurity and emergency response protocols. For example, there is no clear framework on how guidance services should act in the event of a data breach or cyber-attack. Other important gaps include the lack of mandatory cybersecurity trainings for parents and the lack of detailed crisis management plans for cyber-victimized students. In addition, the lack of measurement and assessment tools on issues such as social media and gaming addiction is noteworthy.

The Ministry of National Education Regulation on Preschool Education and Primary Education Institutions was updated and published on February 20, 2021. The Ministry of National Education Regulation on Secondary Education Institutions was updated on September 7, 2021. The regulations on cybersecurity and the use of technology were revised in line with MoNE's digital transformation policies after 2021.

Both regulations include important regulations taking into account the reflections of digital transformation in education. While the preschool and primary education regulations prioritize providing students with the basic skills of digital literacy, the secondary education regulation places special emphasis on the ethical use of technology. Both regulations include general provisions on the protection of student data and address issues such as cyberbullying within the scope of guidance services. In particular, the specification of rules for the use of digital content in project assignments and regulations on game-based learning tools stand out as approaches in line with the requirements of the age.

However, both regulations lack concrete policies on cyber security. The lack of technical details such as school network security, device management and software updates are noteworthy. Critical issues such as procedures to be followed in the event of a cyber-attack, mandatory cybersecurity trainings for teachers and administrators, and a digital security commitment letter are not included in the regulations. In addition, the lack of a clear definition of the responsibilities of parents and students is an important deficiency that may lead to gaps in implementation. This increases the risk of schools being vulnerable to cyber threats.

The Artificial Intelligence in Education Policy Document and Action Plan (2025-2029) gives significant attention to cyber security and data security in the integration of artificial intelligence (AI) technologies into the education system. The document emphasizes critical issues such as student data protection, ethical AI use, and transparent algorithm management, and requires AI tools to comply with security standards. In particular, identifying MoNE-approved AI applications and requiring these tools to be KVKK compliant is an important step in protecting student privacy. In addition, training programs are envisaged for teachers to gain AI literacy and cybersecurity awareness. The Action Plan's objectives such as the preparation of a "Safe AI Usage Guide" and the dissemination of digital ethics trainings in schools stand out as positive approaches.

However, the policy document and action plan do not detail concrete response protocols for immediate cyber risk scenarios (e.g. data breaches or algorithm manipulation of AI systems). There is a lack of clear safeguards for risks that teachers and students may face, such as deepfake, automated data collection or privacy violations from AI-enabled monitoring tools. Furthermore, restrictions or oversight mechanisms for the use of third-party AI applications (e.g. ChatGPT, Midjourney) in schools are not sufficiently defined. Another shortcoming is the lack of concrete steps to raise awareness of parents on AI and cybersecurity. The Action Plan does not include enforceable mechanisms such as a cyber security budget or school-based AI auditors.

Student Level Findings

The Regulation on National Education Directorates (2025) takes important steps for the digital safety of students, requiring the installation of content filtering systems on school internet networks. Students will be able to study in a safe digital environment by blocking access to harmful websites on school Wi- Fi. In addition, regulations on the protection of personal data in systems such as e-School secure grade information and attendance records. The obligation for school administrations to audit cyber security measures is also a positive development in terms of students' data security.

However, the regulation does not fully meet the daily digital needs of students. Since the rules

for connecting to the school network with personal devices (phone/tablet) are not clearly defined, security gaps may occur. It does not clearly define how students should proceed in case of cyberbullying or data breach. In addition, there are no concrete standards for the timeliness of the technology infrastructure in schools and its resistance to cyber-attacks. Regulations to facilitate students' access to cyber security trainings are also not included in the regulation.

The MoNE Guidance Services Directive (2017) provides important protective measures against the risks students face in the digital world. Guidance counselors are obliged to support students in combating cyberbullying, enabling victimized students to receive psychological support. Digital citizenship trainings provide students with basic skills such as safe internet use, protection of personal data and social media ethics. In addition, the foreseeable work to be done on digital addiction helps students develop healthy habits of using technology.

However, the directive is insufficient against current digital risks. It does not specify how guidance services will be carried out on issues such as cyber fraud, account security, artificial intelligence ethics that students may encounter. It does not define concrete steps to be followed in emergency situations (e.g. if a student's social media account is hacked) . Furthermore, there is no obligation for regular cybersecurity trainings for parents, resulting in weak family-school cooperation. The directive does not include up-to-date measures to address next-generation risks that students face in digital environments.

The Ministry of National Education Regulation on Preschool and Primary Education Institutions provides basic protective measures for the digital safety of preschool and primary school students. By setting safety standards for course materials and educational materials, students are prevented from being exposed to age-inappropriate content. Limiting the use of technology in preschool education protects young students from digital risks. In addition, the sharing of student data is controlled through parental consent mechanisms.

The Ministry of National Education Regulation on Secondary Education Institutions contains more detailed regulations on students' use of technology. It sets out rules for the safe use of school networks, rules for the use of digital tools for educational purposes and ethical principles in electronic communication. Standards for the use of technology in student projects have been introduced, ensuring academic integrity and protection of intellectual property rights. In addition, intervention protocols for guidance services in cyberbullying cases have been established.

However, the Regulation on Preschool and Primary Education Institutions of the Ministry of National Education does not contain sufficient regulations for current digital risks that preschool and primary school students may face. There are no concrete standards for data security, especially in educational applications and game-based learning platforms. Procedures to be followed in cases of cyberbullying against young students are not clearly defined. Furthermore, digital literacy training for parents is not mandatory.

The Ministry of National Education's Regulation on Secondary Education Institutions fails to fully address the contemporary digital risks faced by secondary school students. Ethical rules and data security standards for the use of artificial intelligence applications in education are lacking. Security protocols that students must follow when connecting their personal devices to the school network are not detailed enough. Moreover, the integration of digital literacy trainings into the curriculum and measurement and evaluation mechanisms are insufficient.

Regulations for students are mainly found in the Regulation on Primary and Secondary Education Institutions, Guidance Services Directive and the TRT-EBA co-production "Safe Internet Use". These documents state that students should exhibit ethical behavior in digital environments, protect their personal data and avoid risky content online.

However, there is no explicit regulation that students are subjected to a systematic training program on digital security. Differentiation of educational content according to age level, measurement of effectiveness and pedagogical measures to be taken against threats such as cyberbullying are not systematically defined. Moreover, a policy on the integration of parental involvement in the digital safety process and strategies to support digital supervision habits at home are not included in the documents.

The findings of this study show that cybersecurity practices in primary and secondary education institutions in Türkiye are defined at the level of technical guidelines, but are not supported by pedagogical and cultural integrity at the level of teachers and students. Existing documents include elements such as encryption, content filtering and logging to protect IT infrastructure, but provide limited information on how these policies are implemented and monitored in schools.

In particular, the absence of basic security measures such as MFA is inconsistent with contemporary cybersecurity standards. International standards emphasize that multi-factor authentication plays a critical role in preventing data breaches (NIST, 2022). The lack of this in Türkiye shows that authentication is still only at the password level.

While digital competency documents for teachers include principles on digital security, they are not supported by mandatory in-service trainings, leaving teachers' knowledge in this area institutionally weak. However, research shows that if teachers have high cybersecurity awareness, students are more likely to develop safe behaviors in the digital environment (Jayatilaka et al., 2021).

At the student level, current regulations refer to digital safety at the ethical and behavioral level, but this is not enough. OECD (2022) emphasizes that digital safety should be among students' basic life skills and recommends that cyberbullying, digital privacy and online safety should be supported by mandatory curriculum content.

In conclusion, current regulations in Türkiye focus on technical security at the organizational level, but fall short in terms of pedagogical approaches to foster a culture of security at the teacher and student level. This leaves not only systems but also individuals vulnerable to digital threats.

Practices confirm that cybersecurity should be addressed with an ecosystem approach (linking institution-teacher-student). The comprehensive cybersecurity culture model envisioned by organizations such as ENISA and UNESCO has not yet been implemented holistically at the K-12 level in Türkiye (ENISA, 2021).

CONCLUSION AND RECOMMENDATIONS

This study presents a thematic analysis of cybersecurity practices in primary and secondary education institutions in Türkiye based on institutional guidelines, teacher competency documents and student- facing policy texts. The findings show that cybersecurity is defined at the technical level, especially in institutional documents, but these practices are not integrated pedagogically at the teacher and student level.

Conclusions

At the institutional level, MoNE's recent regulations and policy documents (2023-2025) provide a critical framework for schools' cybersecurity infrastructure. The most notable development at the institutional level is the introduction of mandatory content filtering systems on school networks and the definition of formal procedures to be followed in the event of a data breach. In particular, the Artificial Intelligence in Education Policy (2025-2029) fills an important gap by

setting data privacy standards in AI applications. However, there are serious shortcomings in the implementation of these regulations. The most important problem is that schools cannot meet basic infrastructure needs such as firewalls and licensed antivirus software due to lack of budget. Moreover, the lack of periodic cyber security audits and inadequate sanctions reduce the effectiveness of policies.

At the institutional level, MoNE Information Security Directive includes detailed regulations on access control, password policies and logging. However, these documents do not include multi-factor authentication (MFA), systematic log analysis and school-based audit mechanisms.

From a teacher perspective, the Law on Teaching Profession (2023) and the Teacher Qualifications (2017) have significantly increased educators' responsibilities for digital security. Teachers are now held directly responsible for the security standards of the digital tools they use in lessons, protecting student data and preventing cyberbullying cases. The Guidance Services Directive imposes a duty on psychological counselors to support cyber-victim students. However, it is seen that teachers do not have the necessary technical knowledge and equipment to fulfill these responsibilities. Inadequate in- service trainings, the lack of IT specialists in schools, and the lack of technical support lines that they can consult in emergencies put teachers in a difficult situation.

At the teacher level, UNESCO and YEGİTEK supported documents define digital security elements. However, the necessity, continuity and evaluation mechanisms of in-service trainings are lacking. In addition, there are not enough measurable outcomes related to digital security among teacher competencies.

Existing regulations provide basic digital protections for students. School internet filters protect students from harmful content, while data security measures in the e-School system protect personal information. The involvement of guidance services to combat cyberbullying is a positive step. However, current digital risks faced by students (deepfake, social engineering, in-game scams, etc.) are not adequately addressed in policy documents. In particular, there are no school-based solution mechanisms for problems experienced on social media and online gaming platforms. In addition, curriculum-based trainings to raise students' awareness on cybersecurity remain insufficient.

At the student level, although personal data protection and guidance principles are included in the regulations, a sustainable and auditable education model on safe internet use, coping with cyberbullying and privacy awareness has not been developed.

In general, cybersecurity culture in the education system in Türkiye exists at the level of technical documents; however, it has not been structured in a sustainable, traceable and measurable manner in the triangle of teachers, students and parents with an ecosystem approach. This study is one of the few studies in the literature that analyzes the education system in the field of cybersecurity not only through the technical structure but also as a multi-layered structure including teacher, student and institutional dimensions. It also makes a critical contribution to the literature by making the policy- practice gap visible through document analysis.

Policy and Practice Recommendations

Creating an effective cybersecurity culture in educational institutions is a systematic process that requires multidimensional and inter-stakeholder collaboration. In this context, the following recommendations are offered to address the shortcomings in current policies and practices. These recommendations, detailed below, aim to bring holistic solutions to the cybersecurity challenges faced by the Turkish education system in the digital transformation process.

Policy and Legislation Development;

- MoNE Cyber Security Framework Document should be prepared and its implementation should be made mandatory in all schools.
- Minimum security standards should be set for all technologies to be used in education by creating an Artificial Intelligence and Digital Tool Usage Guide.
- Multi-factor authentication (MFA) should be implemented in systems such as EBA, MEBBİS and e-School. This measure is the main layer of security against identity theft, password leakage and social engineering attacks (NIST, 2022)
- A cybersecurity commitment letter should be added to school regulations, and the digital rights and responsibilities of students and parents should be clearly defined.

Within the scope of Strengthening Institutional Capacity;

- Cyber Security Units should be established within each provincial directorate of national education, and regular audits and technical support should be provided to schools.
- A special cyber security budget should be allocated to schools and basic infrastructure needs such as firewalls and encryption software should be met.
- School Cyber Security Teams (IT teachers, counselors, administrators) should be formed and emergency response protocols should be prepared.
- A functioning "School SOME" unit should be established in each school under the coordination of the IT officer or IT teacher; coordination procedures with ICTA and USOME should be defined.

Within the scope of Teacher Training and Support Mechanisms;

- Mandatory cybersecurity certification programs should be implemented for all teachers, and at least 20 hours of training per year should be required.
- MoNE Digital Security Guide should be prepared and the risks that teachers may face and solutions should be explained with case studies.
- At least one Digital Security Officer should be assigned to each school and these teachers should be given additional pay.
- Themes such as digital security awareness, data privacy, content filtering and dealing with online threats should be integrated into all in-service training modules. At the end of the trainings, success evaluations should be made and recorded in the professional development portfolio.

Within the scope of Student and Parent Focused Solutions;

- Digital Citizenship and Security Course should be added to the curriculum and students' skills should be developed through practical trainings.
- Cyber Security Games and Simulations should be developed to enable students to learn interactively.
- Safe Digital Life Trainings for Students should be standardized and monitored.
- Digital Literacy Programs for parents should be organized and school-family cooperation should be strengthened.

Technology and Collaboration Initiatives;

- A Digital Security in Education Research Center should be established in cooperation with MoNE, ICTA and TÜBİTAK.
- Free security software packages should be prepared for schools and a technical support line should be established.

- Cyber Security Competitions should be organized to increase the motivation of students and teachers.

Monitoring and Evaluation;

- A Digital Security Index should be developed to measure the cyber security status of schools.
- Annual Cyber Security Status Reports should be published and improvements should be monitored.
- Cyber Security Excellence Awards should be given to reward successful practices.

Strengthening the cybersecurity infrastructure is no longer a choice, but a necessity for the digital transformation of Türkiye's education system to proceed in a healthy way. The policy, institutional capacity, teacher training and student-oriented recommendations presented in this study aim to create a holistic security ecosystem. In particular, recommendations such as the MoNE Cybersecurity Framework Document, School SOME units and digital citizenship courses are in line with international standards while responding to local needs. It should not be forgotten that an effective cybersecurity strategy can be realized not only with technological investments but also with the active participation of teachers, students and parents.

In today's world of accelerated digitalization in education, cybersecurity has become an integral part of the quality of education. The steps to be taken in line with the findings and recommendations of this study will not only meet a technical requirement, but will also contribute to Türkiye's digital education vision. In the coming period, it is clear that investments in cybersecurity will improve educational outcomes, increase students' digital competencies and strengthen the country's human resource potential. In this context, an integrated cybersecurity approach to be implemented with the cooperation of all stakeholders will play a decisive role in ensuring that the Turkish education system meets the requirements of the digital age.

References

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal,* 9(2), 27–40. https://doi.org/10.3316/QRJ0902027

ENISA. (2021). Cybersecurity maturity assessment framework for the public sector. https://www.enisa.europa.eu/publications

ENISA. (2025). NIS2 implementation guidelines for education sector. https://www.enisa.europa.eu

European Parliament & Council. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity. https://eur-lex.europa.eu

Ibrahim, A., Li, Y., & Watson, R. (2024). A systematic review of cybersecurity education in K–12 curricula worldwide. *ResearchGate*. https://www.researchgate.net/publication/

Jayatilaka, G., Ranaweera, K., & Wijesundara, N. (2021). Digital responsibility and child online safety in education. *International Journal of Digital Education*, 14(3), 45–60.

MEB (Milli Eğitim Bakanlığı). (2023). Bilgi ve Sistem Güvenliği Yönergesi. https://meb.gov.tr

MEB. (2023). 2023–2025 Stratejik Planı. https://sgb.meb.gov.tr

OECD. (2018). Digital Government Review of Brazil: Towards the Digital Transformation of the Public Sector. https://www.oecd.org

Rayavaram, P., Kumari, S., & Bajaj, R. (2023). Visual cryptography curriculum with Scratch: A pilot implementation. *arXiv*. https://arxiv.org/abs/2301.12345

Tasay, D., & Başaran-Demir, M. (2025). Öğretmenlerin siber güvenlik farkındalık düzeyleri: Bir nitel analiz. *Eğitim ve Teknoloji Dergisi*, 15(1), 101–120.

Yalçınkaya, B. (2023). Eğitim kurumlarında dijital güvenlik sorumluluğu ve veri etiği. A*çıköğretim Uygulamaları ve Araştırmaları Dergisi*, 9(2), 56–72.

Zdrnja, B. (2024). Navigating NIS2: Implementation challenges for the public sector. *SANS Institute Report*. https://www.sans.org