AMERICAN JOURNAL OF EDUCATION AND LEARNING
ISSN: 2996-5128 (online) | ResearchBib (IF) = 10.91 IMPACT FACTOR
Volume-4| Issue-4| 2026 Published: |30-04-2026|

FOSTERING A CULTURE OF INFORMATION SECURITY IN SCHOOLS: AGE-APPROPRIATE TEACHING METHODS, ACTIVE LEARNING TECHNIQUES AND EFFECTIVENESS ASSESSMENT

https://doi.org/10.5281/zenodo.19996615

Jiyanbayeva Dilnaz Qosimbay qizi
2nd year of Master's degree
Nukus state pedagogical institute named after Ajiniyaz
(Republic of Karakalpakstan, Nukus)

Abstract

The present article proposes a systematic framework for the pedagogy of imparting foundational competencies in information security to schoolchildren within the digital environment. The document delineates the objectives and principles of education, encompassing primary, lower secondary, and upper secondary schools. It elucidates active teaching methodologies and a comprehensive system for evaluating performance. A notable emphasis is placed on the role of the family and interdisciplinary collaboration in cultivating a sustainable culture of safe and responsible online behaviour.

Keywords

information security, digital literacy, teaching methodology, age-appropriate differentiation, case study method, project-based learning, cyberbullying, personal data, media literacy, effectiveness assessment.

INTRODUCTION: In the contemporary era, the lives of many children and young people are predominantly shaped by the digital environment. The internet offers a vast array of opportunities for learning, communication and creative self-expression. However, it is important to acknowledge the potential risks associated with the internet, including cyberbullying, fraud, the spread of harmful content and the leakage of personal data. It is evident that schoolchildren who frequently utilise the internet frequently demonstrate an absence of adequate digital literacy and critical thinking skills, which is a prerequisite for the identification of potential risks and the implementation of adequate protective measures.

In this regard, the education system should not restrict children's access to digital resources; rather, it should equip them with the ability to navigate the digital space safely and effectively. The fostering of a culture of information security is becoming an integral part of the functional literacy of the modern individual. The present article aims to systematise methodological approaches to

introducing schoolchildren to the basics of information security. In addition, it proposes a structured working model for teachers.

METHODS: The objective of the programme is to furnish students with a comprehensive body of knowledge, practical skills and competencies, as well as values that ensure responsible and safe behaviour in the digital environment.

In order to achieve this aim, a set of objectives has been identified, which are then grouped into three categories that are interrelated.

1. Educational objectives
2. The following developmental objectives are to be considered:
3. Formative objectives

The following methodological principles must underpin teaching:

The issue of age-appropriateness is a pertinent one in this context. The content and teaching methods employed are selected with consideration for the psychophysiological and cognitive characteristics of students at each stage of education.

The practical focus of the programme is evident in the manner in which theoretical concepts are reinforced through a variety of exercises, case studies and the simulation of real-life situations.

– Continuity and Progression: The development of information security competencies is carried out consistently across all stages of school education, with the content becoming progressively more complex.

Interactivity and dialogue-based learning are pivotal components of the teaching methodology. The pedagogy is structured as a collaborative search for solutions through discussions, problem-based tasks and collective reflection.

Interdisciplinarity is evident in the integration of elements of information security into various academic disciplines, including computer science, health and safety, social studies, law, and literature. This integration extends to primary school level, signifying a comprehensive approach to education.

The establishment of a partnership with families is of paramount importance. Parents are regarded as pivotal partners in the educational process; systematic awareness-raising and engagement with families are essential components of this endeavour.

Pedagogical Approaches for Primary Education (Years 1–4)

In the primary school curriculum, children commence the active engagement with digital resources through play, encompassing games, cartoons and children's social media platforms. Play is the primary activity, and as such, teaching methods must take into account the inherently playful nature of learning.

The following topics are of particular significance:

- The notion of the internet and the opportunities afforded by the digital environment, as well as the potential risks associated with it.

In the context of online interactions, it is imperative to exercise caution when disclosing personal information, such as one's name, address, telephone number, and school, to individuals with whom one has no prior personal acquaintance.

The creation of passwords is a process that adheres to a set of simple guidelines. These guidelines encompass the creation and storage of passwords, as well as the utilisation of mnemonics to facilitate their memorisation. To illustrate this point, one may consider the password to be analogous to one's personal toothbrush.

The following discourse will address the potential risks associated with communication between individuals who are not acquainted with each other. The discussion will utilise real-world analogies to provide a contextual framework for the online environment.

In the context of online abuse, the following steps are recommended: first, the abuse should be halted; second, the abuser should be blocked; and third, a trusted adult should be informed.

Advertising is a critical field that requires careful consideration. When dealing with pop-ups and buttons that are designed to attract the viewer, caution should be exercised.

The following is a synopsis of the fundamental principles that govern copyright law. It is essential to exercise due respect for the intellectual property of others and to obtain explicit consent before utilising their images or texts.

The methodology should ensure the material is accessible, rely on visual aids and gamification, and provide for the regular involvement of parents in the educational process.

Guidelines for secondary schools (Years 5–9)

Adolescence is characterised by active use of social media, messaging apps, blogging and participation in online games. For pupils at this stage, issues of social identity and recognition are critically important, which increases vulnerability to cyber threats, grooming and the development of internet addiction (Smith, 2023). The methodology must encompass the emotional and social motivations of adolescents and be grounded in practice-oriented approaches.

The following thematic areas are of particular significance: personal data and privacy. A thorough investigation into the privacy settings on social media platforms was conducted, encompassing an examination of the risks associated with the dissemination of geotags and photographs. This investigation yielded practical recommendations for the mitigation of personal information disclosure.

The following issue is to be considered: the prevention of phishing and online fraud. The following topics will be explored in this study: the hallmarks of fraudulent emails and fake websites; and methods for verifying sources and behaving safely when faced with suspicious requests.

The following essay will explore the phenomenon of cyberbullying and the countermeasures that have been developed in response to it. The following step-by-step guidelines are to be followed by victims and witnesses:

- Support strategies and mechanisms for seeking help are to be discussed.
- The psychological consequences of online aggression are to be examined.

The concept of an online reputation is of particular relevance in this context. It is imperative to comprehend the long-term ramifications of digital publications with regard to university admissions and employment prospects. The development of competencies in the management of digital footprints is also essential.

The presence of malicious software is indicated. The following topics will be covered: the methods by which infection occurs, the signs of compromised devices, and basic anti-virus protection measures.

The following aspects are of particular significance in this context: firstly, the capacity for critical thinking, and secondly, the ability to exercise media literacy. The following techniques will be employed to verify the accuracy of information, recognise fake news and identify manipulative techniques:

- Practical exercises in verifying sources
- Legal framework. The following issues are to be considered in relation to the liability for unlawful online activities, the legal consequences of the distribution of prohibited content and insults:

The present study will examine the relationship between psychological well-being and other factors. The following issues are to be considered: the question of internet addiction, and the principles of digital balance and self-regulation.

The pedagogical approach should integrate analytical work with experiential skill-building, provide emotional support and involve parents in educational initiatives.

Methodological recommendations for upper secondary school (Years 10–11)

It is widely acknowledged that upper secondary school pupils have reached a level of maturity that renders them competent digital users, preparing them for independent life. In light of this, it is recommended that educational work focus on issues of financial security, professional digital hygiene and civic responsibility online.

The following thematic areas are of particular significance:

1. Financial security. It is imperative to acknowledge the necessity of adhering to secure practices when engaging in online shopping and internet banking. In this regard, it is essential to recognise the methods employed by fraudulent entities to perpetrate financial scams and to identify fraudulent offers.

The following text is concerned with practical cryptography and communication security. In order to ensure the protection of personal correspondence and data, it is recommended that users employ virtual private networks (VPNs), two-factor authentication, and fundamental encryption methods.

Digital hygiene in professional life is of paramount importance.

The following rules must be observed when using work accounts:

- Access management
- Maintaining confidentiality when interacting with employers and colleagues

It is imperative to ensure the security of interactions with government services. The following recommendations are provided for the safe use of government and public service portals.

The following essay will explore the concepts of cybercrime and criminal liability. This study will undertake an exhaustive examination of the legal ramifications arising from illicit online activities, complemented by empirical case studies that illuminate law enforcement practices.

The following essay will explore the notion of information security, both in the context of individuals and in that of the state. The following essay will provide a comprehensive overview of the fundamental principles that underpin the countering of ideological extremism, propaganda and disinformation.

The following discourse pertains to the notion of digital identity and reputation management, with a particular focus on the deliberate cultivation and preservation of a professional online persona.

The secondary school curriculum should foster independence, critical risk assessment and a readiness for responsible digital behaviour in adult life, combining theoretical depth with practical applicability.

An effective methodology involves a transition from a predominantly lecture-based format to active learning methods, which enable the practical development of skills and critical analysis of situations.

The case study method involves the analysis of real or simulated incidents involving data breaches, cyberbullying and fraud. The students are tasked with the analysis of errors, the identification of the root causes of the incident, and the formulation of a phased response and prevention plan.

The project work will entail the implementation of social initiatives, which will include the following:

- The establishment of a school cyber patrol
- The organisation of a digital literacy week
- The production of video materials containing safety recommendations Projects facilitate the development of research and communication skills, while ensuring the practical relevance of knowledge.

The utilisation of business games entails the emulation of the operations of an information security department, or the enactment of incident response scenarios. The utilisation of role-play scenarios in training programmes has been demonstrated to engender the development of teamwork skills, effective role allocation and the capacity for expeditious decision-making.

The training sessions are designed to be targeted and to develop specific skills. These include countering bullying, managing emotional states during information overload, and safe behaviour practices when dealing with suspicious messages.

The organisation of reasoned discussions on controversial issues in the digital environment is of paramount importance. The act of debating helps to develop critical thinking skills, the ability to construct arguments, and an understanding of legal and ethical considerations.

The utilisation of simulators and online training tools constitutes a valuable method of honing skills in threat recognition and online safety. These tools offer specialised platforms that provide interactive scenarios and game-based tasks, which facilitate the development of these critical competencies.

It is evident that, in the absence of systematic involvement from families, educational institutions will encounter limitations in their efforts to promote digital safety. It is incumbent upon educational institutions to establish ongoing educational and advisory work with parents.

The organisation of parent meetings on the topic of internet safety is recommended. The organisation holds regular meetings for the purpose of elucidating current risks, demonstrating practical privacy settings and providing recommendations on the monitoring of children's digital activity.

The provision of consultations with psychologists and IT specialists is an integral component of the service. The organisation of consultations, both face-to-face and remote, is conducted for parents with the aim of analysing specific situations and providing professional advice on prevention and response.

The following information resources are available for families. The creation and maintenance of contemporary materials is imperative, encompassing the development of informative leaflets and brochures, in addition to the establishment of a dedicated section on the school website that provides guidance on emerging threats and the utilisation of protective tools.

The establishment of trusting relationships and the judicious utilisation of monitoring mechanisms are of paramount importance. It is recommended that parents establish an open dialogue with their child so that they can report any problems. Parental control tools should be used as a means of support and guidance, rather than as a mechanism for total restriction.

RESULTS AND DISCUSSION: The evaluation of the efficacy of initiatives designed to enhance information security skills should not be confined to formal assessments. It is imperative to undertake a thorough evaluation of the observed changes in students' behaviour and the extent to which they have acquired the pertinent competencies, incorporating several complementary components.

The following text concerns the knowledge component. The evaluation of this domain is conducted through a series of assessments, encompassing tests, surveys and quizzes. These instruments are meticulously designed to ascertain the extent of mastery concerning fundamental rules and procedures that are pivotal for ensuring safe online conduct. The utilisation of such tools facilitates the documentation of theoretical knowledge gaps, thereby enabling the identification of deficiencies in understanding of risks and protection methods.

The following text concerns the practical component. The programme is designed to emphasise the acquisition of practical skills, encompassing the observation of pupils' behaviour within the school's digital environment, the completion of practical tasks (e.g. the verification of URLs for indications of phishing), the presentation of project work, and the demonstration of response algorithms in simulated scenarios. This section is designed to evaluate the ability to apply knowledge in real-life or near-real-life conditions.

The following component is of an inspirational and values-based nature. The objective of this study is to ascertain the attitudes of students towards security issues. To this end, a series of questionnaires will be administered to ascertain the students' value systems. Surveys will also be conducted to ascertain their motivations. Finally, reflective sessions will be held after classes to discuss the findings. With the students' consent, an anonymised analysis of their digital footprint may be conducted to examine self-presentation practices and risk-inducing behaviour.

CONCLUSION: The induction of schoolchildren into the rudiments of information security constitutes a multifaceted and ongoing process that necessitates a systematic approach. The proposed methodology, grounded in the principles of age-appropriateness, practical focus and interdisciplinary integration, is designed to achieve two primary objectives: the transfer of knowledge and the cultivation of a sustainable internal culture of safe and responsible behaviour in the

global digital environment. Achieving sustainable results is only possible through close collaboration between teachers, parents and pupils, who must act as active participants in the process of ensuring their own digital safety. This contributes to the protection of every child and to the creation of a safer and more ethical digital space for society as a whole.

REFERENCES:

1. Proekt «Izuchi Internet - upravlyay im!» [Elektronniy resurs]. - URL: httpsy/igra-internet.rf/ (Data obrasheniya: 25.11.2025)
2. Metodicheskie rekomendasii po realizasii meropriyatiy po povisheniyu pravovoy gramotnosti detey, roditeley i pedagogicheskix rabotnikov, uchastvuyushix v vospitanii detey. / Ministerstvo prosvesheniya RF. - M., 2022.
3. Kengesbayevich, R. M. (2025). INDIVIDUAL PERSONALITY TRAITS OF JUNIOR PUPILS IN SCHOOLS OF EDUCATION. In *International Conference on Adaptive Learning Technologies* (Vol. 13, pp. 24-25).
4. Kengesbayevich, R. M. (2025). ETHNOCULTURAL ASPECTS OF VALUE ORIENTATIONS. *AMERICAN JOURNAL OF EDUCATION AND LEARNING*, *3*(1), 40-43.
5. Liga bezopasnogo interneta. [Elektronniy resurs]. - URL: https://ligainternet.ru/ (Data obrasheniya: 25.11.2025)