AN INCLUSIVE-APPROACH-BASED MODEL FOR DEVELOPING AN INFORMATION SECURITY CULTURE IN PRIMARY SCHOOL STUDENTS

Norqobilova Durdona Ural qizi
Lecturer, University of Information Technologies and Management
E-mail: durdonanorqobilova326@gmail.com
ORCID: 0009-0004-4653-5892
https://doi.org/10.5281/zenodo.23216587

Abstract

This article examines the problem of developing an information security culture in primary school students on the basis of the inclusive education approach. As primary school students increasingly use the internet, mobile devices, digital learning resources and social communication tools in the modern digital environment, developing their skills to search for, select, store and evaluate information safely, and to use it responsibly, is becoming an important pedagogical task.

The article clarifies the content of the concept of "information security culture" and substantiates the pedagogical potential of the inclusive approach in developing it. A model for developing an information security culture in primary school students has also been designed, consisting of target, content, process, inclusive and outcome components.

The model pays particular attention to students' individual abilities, age and psychological characteristics, level of work with information, and special educational needs. The motivational-value, cognitive, practical-activity and reflective components of information security culture are identified, together with their criteria, indicators and diagnostic tools. The article also describes the pedagogical conditions for introducing the model into the primary education process.

Keywords: primary education, information security, information security culture, inclusive education, inclusive approach, digital competence, information culture, primary school student, pedagogical model, digital safety.

INTRODUCTION

Today, the rapid entry of digital technologies into the educational process is fundamentally changing the relationship of primary school students with the information environment. Students are making ever more active use of various electronic learning resources, internet networks, mobile devices, video materials, interactive platforms and communication tools [3;6]. While expanding learning opportunities, this process also increases the likelihood that children will encounter various information risks.

Children of primary school age in particular lack sufficient experience in independently assessing the reliability of information, protecting their personal data, distinguishing dangerous links, understanding the consequences of communicating online with strangers, and anticipating the results of their behavior in the digital environment. For this reason, it is necessary to develop information security skills from the preschool or primary education stage.

This task becomes even more important in inclusive education settings, because inclusive education aims to create equal educational opportunities for all students, regardless of their individual abilities, developmental characteristics and educational needs [9;11].

It follows that, in developing an information security culture in primary school students, it is more appropriate to rely on individual approaches, differentiated instruction, visual and interactive tools, and pedagogical technologies suited to students' abilities than to set a single, uniform requirement for all students.

Aim of the research: to develop a pedagogical model, based on the inclusive approach, for developing an information security culture in primary school students and to determine its pedagogical conditions.

Object of the research: the process of developing students' digital competence in primary education.

Subject of the research: the content, forms, methods and tools of developing an information security culture in primary school students in inclusive education settings.

Research tasks:

– to clarify the content of the concept of "information security culture" from the standpoint of primary education;

– to define the components, criteria and indicators of this culture;

– to develop a pedagogical model based on the inclusive approach;

– to substantiate the pedagogical conditions for implementing the model;

– to design diagnostic tools.

Scientific novelty:

– information security culture has been defined for the primary school student as a four-component structure (motivational-value, cognitive, practical-activity, reflective);

– a separate inclusive component (differentiated tasks, visual, audio and interactive materials) has been introduced into the model;

– teacher–student–parent collaboration has been defined as an integral part of the model;

– a system of criteria and indicators determining the levels of this culture (high, medium, low) has been proposed.

Practical significance: primary school teachers and teachers of inclusive classes can use the proposed model and diagnostic tables in lessons and extracurricular activities.

LITERATURE REVIEW

The problem of information security is one of the important scientific fields taking shape at the intersection of modern pedagogy, psychology and information technology. Whereas the concept of information security was initially associated with technical security and the protection of information resources, today it also covers a person's competence to act safely, consciously and responsibly in the information environment.

In the media and information literacy concept advanced by UNESCO, a person's responsible participation in searching for, using and evaluating information and in creating it is identified as an important competence [1;2].

In the European Commission's DigComp framework, one of the key areas of digital competence is "Safety", which covers protecting devices, ensuring personal data and privacy, safeguarding well-being in the digital environment, and understanding the environmental impact of digital technologies [3].

Scientific studies on inclusive education pay particular attention to adapting the educational process to students' diverse needs, creating equal opportunities in the use of educational resources, applying a differentiated approach, and improving mechanisms of pedagogical support [8; 9; 10; 11].

At the same time, the question of developing an information security culture in primary school students specifically on the basis of the inclusive approach has not been addressed systematically enough in existing research. This circumstance determines the relevance of the present research topic.

RESEARCH METHODOLOGY

The research used systemic, competence-based, student-centered, activity-based and inclusive approaches.

The research methods envisaged were analysis of pedagogical and psychological literature, comparison, generalization, modeling, pedagogical observation, interviews, diagnostic tasks and the pedagogical experiment.

The methodological basis of the research consists of the following principles:

– equality of educational opportunities for all students;
– taking individual educational needs into account;
– suitability to age and psychological characteristics;
– activity orientation;
– practical orientation;
– consistency and continuity;
– creating a safe digital environment;
– collaboration among the student, the teacher and the parent.

THE CONTENT OF THE CONCEPT OF INFORMATION SECURITY CULTURE

In our research, the concept of "information security culture" is interpreted as a primary school student's readiness to behave safely, consciously, responsibly and ethically in the digital and information environment.

A primary school student's information security culture includes the following key skills:

– **Searching for information safely** – searching for the needed information on the internet correctly and being wary of inappropriate resources.

– **Evaluating information** – distinguishing whether information is reliable or suspicious on the basis of simple criteria.

– **Protecting personal data** – not giving strangers information such as name, address, telephone number, passwords or photographs.

– **Digital communication culture** – communicating politely and responsibly with other internet users.

– **Identifying dangerous situations** – recognizing a suspicious link, an unknown message or an approach by a stranger as a danger.

– **Acting correctly when a danger arises** – turning to a parent, a teacher or another trusted adult in a problematic situation.

– **Digital hygiene** – controlling time spent on devices and following the rules of safe use.

A MODEL FOR DEVELOPING INFORMATION SECURITY CULTURE ON THE BASIS OF THE INCLUSIVE APPROACH

As a result of the research, the following model for developing an information security culture in primary school students is proposed (Figure 1, Table 1).

ISSN:2308-5703
Impact factor:13.5 *International Multidisciplinary Online Journal* October, 2026

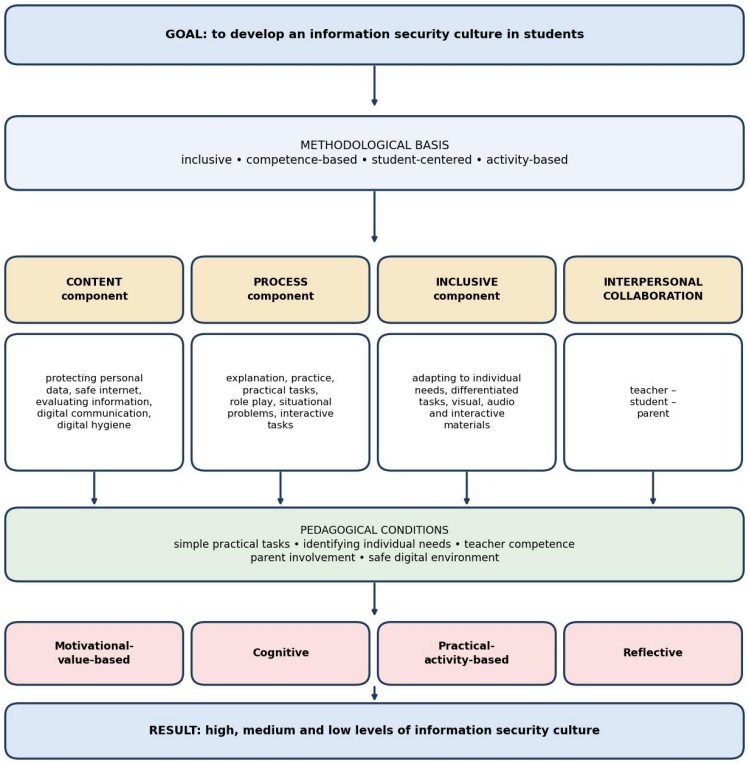

Figure 1. An inclusive model for developing information security culture

Table 1. Structural components of the model

Model component	Content
Target component	Developing an information security culture in students
Methodological component	Inclusive, competence-based, student-centered and activity-based approaches
Content component	Protecting personal data, safe internet, evaluating information, digital communication, digital hygiene
Process component	Explanation, practice, practical task, role play, situational problem, interactive tasks
Inclusive component	Adapting to individual needs, differentiated tasks, use of visual, audio and interactive materials
Interpersonal collaboration	Teacher–student–parent collaboration
Outcome component	High, medium and low levels of information security culture

The target component of the model is directed at developing in students initial knowledge about information security, safe-behavior skills and a responsible attitude.

In the content component, the simple and practical content of information security is determined with the age characteristics of primary school students taken into account.

The process component ensures students' active participation in real or simulated situations. For example, situational tasks such as "An unknown link has arrived. What will you do?", "A stranger asked for your name and photo online. How will you act?" and "Can you tell your friend your password?" can be used.

The inclusive component is an important part of the model and involves taking students' individual abilities and educational needs into account. For example, for some students text-based tasks may be offered, while for others tasks based on pictures, symbols, audio materials or practical demonstrations may be offered [10].

STRUCTURAL COMPONENTS, CRITERIA AND INDICATORS OF INFORMATION SECURITY CULTURE

In our view, it is appropriate to assess the information security culture of primary school students on the basis of the following four components.

1. Motivational-value component

This component expresses the student's attitude toward information security. The student understands the need to protect his or her own and others' personal data.

2. Cognitive component

This component expresses the student's knowledge of information security. It implies knowing, at a level appropriate to his or her age, concepts such as password, personal data, dangerous link, reliable information and online danger.

3. Practical-activity component

This component expresses the student's ability to apply acquired knowledge in real situations. For example, not opening a suspicious message, not giving personal data to strangers, and turning to adults in a dangerous situation.

4. Reflective component

This component expresses the student's ability to evaluate his or her own digital behavior and to recognize his or her mistakes.

The criteria, indicators and diagnostic tools for each component are given in Table 2.

Table 2. Criteria and indicators of information security culture

Component	Criterion	Indicators	Diagnostic tool
Motivational-value	Attitude toward safety	Understands the need to protect personal data; strives to follow safety rules	Interview; picture-based questionnaire
Cognitive	Level of knowledge	Knows the concepts of password, personal data and dangerous link; distinguishes reliable from suspicious information	"True or false?" test; picture-based tasks
Practical-activity	Application of knowledge	Does not open a suspicious message; does not give information to a stranger; turns to an adult when a danger arises	Situational task; role play; pedagogical observation

ISSN:2308-5703

Impact factor:13.5 *International Multidisciplinary Online Journal* October, 2026

Component	Criterion	Indicators	Diagnostic tool
Reflective	Self-assessment	Evaluates his or her own behavior; recognizes and corrects mistakes	"What did I do?" reflection card

Each indicator is scored from 0 to 2 points (0 – cannot perform; 1 – performs with an adult's help; 2 – performs independently). Based on the total score, the students' level of culture is determined according to Table 3.

Table 3. Criteria for the levels of information security culture

Level	Score range	Description
High	13–16	Knows information security rules well, identifies dangerous situations independently, protects personal data and asks adults for help when necessary
Medium	7–12	Knows the basic safety rules, but in some situations needs the support of a teacher or parent
Low	0–6	Does not sufficiently understand the rules, has difficulty distinguishing dangerous from safe situations, and needs external support

In inclusive classes, the form of assessment (oral, picture-based, audio or based on practical demonstration) is adapted to the student's needs, while the assessment criteria remain unchanged.

PEDAGOGICAL TOOLS USED IN INCLUSIVE EDUCATION SETTINGS

In developing an information security culture, using the same method for all students may not produce the expected result. It is therefore appropriate to present learning materials in different forms. In particular:

– pictures and pictograms;
– short video clips;
– audio explanations;
– comics;
– interactive games;
– role-playing games;
– situational tasks;
– tasks delivered via QR codes;
– digital tests;
– "True or false?" exercises;
– the "Find the danger" game;
– "What do I do?" situational exercises.

For example, on the topic "Safe internet", students are presented with three situations:

Situation 1: a stranger asked the student for his or her home address.

Situation 2: a friend asked the student to tell him or her the password.

Situation 3: the student received a message inviting him or her to click on an unknown link.

For each situation, the student chooses an answer such as “safe”, “dangerous” or “need to ask an adult for help”. Such tasks serve to develop not the student’s theoretical knowledge but the competence of making practical decisions.

PEDAGOGICAL CONDITIONS FOR IMPLEMENTING THE MODEL

To ensure the effectiveness of the proposed model, the following pedagogical conditions must be created:

– first, systematically including simple and practical tasks related to information security in the content of primary education;

– second, identifying students’ individual educational needs and adapting learning materials;

– third, developing teachers’ competencies in digital safety and inclusive pedagogy;

– fourth, involving parents in the educational process;

– fifth, creating a safe digital environment at school;

– sixth, organizing information security activities on the basis of practical and situational tasks rather than limiting them to the transmission of theoretical information.

RESULTS AND DISCUSSION

The theoretical analysis of the research shows that it is not sufficient to consider the issue of developing an information security culture in primary school students only within the framework of informatics or digital technologies. This process is closely connected with personal upbringing, moral development, communicative culture, media literacy and inclusive education.

The main advantage of using the inclusive approach is that it makes it possible to present knowledge about information security in a form that is understandable and accessible to all students.

The expected results of the model are described by the three levels given in Table 3: high, medium and low. In this respect, developing an information security culture should be regarded not as a one-off event but as a pedagogical process that is carried on consistently at all stages of primary education.

CONCLUSION

Developing an information security culture in primary school students is one of the pressing pedagogical problems in the context of digital education. As students’ opportunities to use the internet and digital technologies expand, the need to develop their knowledge and skills in information security also grows.

As a result of the research, a model for developing an information security culture based on the inclusive approach was proposed. The model consists of target, methodological, content, process, inclusive and outcome components. Criteria, indicators and diagnostic tools were developed for the four components of this culture.

In this model, taking the student’s individual abilities into account, adapting the educational content, using visual and interactive tools, teaching on the basis of practical situations, and ensuring teacher–student–parent collaboration were defined as the main pedagogical conditions.

Thus, information security education organized on the basis of the inclusive approach serves to develop in primary school students not only protection from digital risks but also the competence to use information consciously, responsibly and ethically.

In the future, promising directions of the research include testing the effectiveness of the proposed model through experimental work, refining the diagnostic criteria, and developing methodological support aimed at forming information security in primary school students.

REFERENCES

1. Republic of Uzbekistan. Law "On Education". No. ZRU-637, 23 September 2020. (in Uzbek)
2. Resolution of the President of the Republic of Uzbekistan "On approving the Concept for the development of inclusive education in the Republic of Uzbekistan". – 2020. (in Uzbek)
3. Decree of the President of the Republic of Uzbekistan "On approving the 'Digital Uzbekistan – 2030' Strategy". – 2020. (in Uzbek)
4. Ministry of Preschool and School Education of the Republic of Uzbekistan. State educational standards of general secondary education and related regulatory and methodological documents. (in Uzbek)
5. Khalikov, A. K. (2023). Scientific-theoretical foundations of social adaptation of young graduates with visual impairments in life. Mental enlightenment scientific-methodological journal, 253-264.
6. Qahramonovich, X. A. (2023). Pedagogical cooperation in implementing the independent-life social adaptation of young graduates with visual impairments. Science and innovation, 2(special issue 12), 561-563. (in Uzbek)
7. Qahramonovich, X. A. (2026). Vocational guidance of young people in the context of inclusive education. Shokh articles library, 1(1), 563-566.
8. Khalikov, A. (2024). Professional faults in the activity of a teacher. Science and innovation, 3(b9), 61-63.
9. Khalikov, A. (2023). Principles and methods of increasing teaching excellence in the modern educational space. Science and innovation, 2(b11), 164-167.
10. Khalikov, A. (2023). Communicative methods of communication with students. Science and innovation, 2(b11), 491-494.
11. Khalikov, A. (2023). The set of abilities that characterize the "pedagogical skill" of a teacher. Science and innovation, 2(b11), 160-163.
12. Khalikov, A. K. (2017). Methodical bases of increasing educational activities in legal education of students with limited vision. Eastern european scientific journal, (4), 69-71.
13. UNESCO. Media and Information Literacy: Policy and Strategy Guidelines. – Paris: UNESCO, 2013.
14. UNESCO. Global Media and Information Literacy Assessment Framework: Country Readiness and Competencies. – Paris: UNESCO, 2013.
15. European Commission. The Digital Competence Framework for Citizens: DigComp 2.2. – Luxembourg: Publications Office of the European Union, 2022.
16. European Commission. Digital Education Action Plan 2021–2027. – Brussels: European Commission, 2020.
17. UNICEF. Policy Guidance on AI for Children. – New York: UNICEF, 2021.
18. Livingstone S., Haddon L., Görzig A., Ólafsson K. Risks and safety on the internet: The perspective of European children. – London: EU Kids Online, 2011.