

Comparative analysis of information security education in the National Core Curricula of Austrian and Slovakian primary schools and grammar schools

Bence Pásztor^{*1}, Eszter Jeso², Gergely Kocsis³ and Dávid Demeter⁴

¹Department of Informatics, J. Selye University, Slovakia, EU

²Independent Researcher, Slovakia, EU

³Department of Informatics, J. Selye University, Slovakia, EU

⁴Department of Informatics, J. Selye University, Slovakia, EU

**(pasztor.bence@student.ujs.sk) Email of the corresponding author*

(Received: 26 January 2026, Accepted: 05 February 2026)

(6th International Conference on Recent Academic Studies ICRAS 2026, January 27-28, 2026)

ATIF/REFERENCE: Pásztor, B., Jeso, E., Kocsis, G. & Demeter, D. (2026). Comparative analysis of information security education in the National Core Curricula of Austrian and Slovakian primary schools and grammar schools, *International Journal of Advanced Natural Sciences and Engineering Researches*, 10(2), 14-19.

Abstract – The role of information security education is becoming increasingly important in primary and grammar education, as young people regularly use the internet in their everyday activities for learning, communication, and entertainment. The widespread use of digital devices and online platforms exposes students to various risks, such as data misuse, cyberbullying, online fraud, and privacy violations, which makes the development of information security awareness an essential educational objective. Consequently, schools play a key role in equipping students with the necessary knowledge and skills to navigate the digital environment safely and responsibly.

The aim of this study is to explore how information security education is reflected in the National Core Curricula of two Central European countries, Austria and Slovakia. The research focuses on examining the place and emphasis of information security-related content within the formal education systems of these countries. In the course of the study, we review and compare the number of information technology lessons provided at both primary and secondary school levels. In the case of Austria, the analysis concentrates on general secondary schools, while in the case of Slovakia, it is based on the national core curriculum for grammar schools.

The primary objective of the study is to demonstrate the extent to which information security education is integrated into the official curriculum frameworks of the two countries, as well as the forms in which it appears. By doing so, the research seeks to assess how effectively the education systems prepare students to recognize and respond to online threats.

Keywords – Information security, National Core Curriculum, Education, Slovakia, Austria

I. INTRODUCTION

Digitalisation is fundamentally transforming the learning environment and expectations of students at all levels of education. The use of digital devices, access to online information sources, and network communication already play a decisive role in primary schools, while students are becoming active

participants in the online space at an increasingly early age and with increasing frequency [1], [2]. According to international data, internet use among children is extremely widespread and continues to grow: for example, in OECD countries in 2021, 93% of 10-year-olds had an internet connection, while more than 95% of 15-year-olds had internet and mobile devices at home, and the frequency of digital device use has increased over the past decade [3]. At the same time, the risks of the digital space and issues related to information security are also coming to the fore. The growth of online presence in education and everyday life not only opens up opportunities—such as quick access to information and new forms of learning—but also poses increasingly complex challenges in terms of data protection, online harassment, personal information protection, and cyber threats. This is supported by the literature, which points out that children's use of the internet increases security and privacy risks, while reinforcing the need for conscious and safe digital behaviour [4]. It is extremely important to prepare students for safe internet use at an early age, as they are becoming active participants in the online space at an increasingly young age. This preparation does not only mean imparting technical knowledge but also enabling students to critically evaluate online information, recognise risks, and protect their personal data. In order to effectively acquire these skills, awareness training must be systematically integrated into compulsory education as part of the state-issued curriculum.

The aim of this study is to explore how information security is addressed in the national core curricula for computer science in Slovakia and Austria. The analysis covers both primary and secondary school levels, examining how curriculum documents promote conscious internet use among students. The research maps out what information security knowledge students need to acquire at what age, according to the national core curricula.

II. MATERIALS AND METHOD

During the research, we used document analysis methods to map how information security is presented in national core IT curricula in Austria and Slovakia. During the study, we paid particular attention to the depth and manner in which information security is presented. In our research, we relied solely on the national core curricula for primary schools and general secondary schools in Slovakia and for primary schools and secondary schools (*allgemeinbildende Schulen*) in Austria and did not take into account the educational material prescribed for other types of schools.

During the analysis, we examined the following key aspects: the presence of digital security and data protection topics in each grade; the competency goals and development requirements defined by the curriculum that promote the development of conscious and responsible internet use; and the gradual progression and age-appropriate level of knowledge from the lower grades of elementary school to grammar school.

The research was based on officially published national core curricula, which were available on the websites of the official ministries of education. A comparative analysis of the documents made it possible to identify the emphases and differences in the national core curriculum of Slovakia and Austria with regard to information security education.

A. Limitations of the research

During the research, the different structures of the compared education systems had to be taken into account, which imposed limitations on the interpretation of the results. Primary school in Slovakia lasts nine years, with lower primary school covering grades 1–4 and upper primary school covering grades 5–9. In Austria, on the other hand, primary school lasts four years, after which students continue their studies in the lower grades of general secondary school, which lasts four years. The upper grades of general secondary school also last four years.

A further limitation of the research is that in Austria, elementary school students learn computer science integrated into other subjects, such as German, German as a second language, mathematics, art, technology, and design, where they may encounter computer science concepts.

Table 1. Number of IT lessons at various levels of education in Slovakia [10], [11], [12] and Austria [8], [9]

		Slovakia			Austria
Primary school	Lower primary school (1-4. grades)	2 lessons (0-0-1-1)	Primary school	(1-4. grades)	-
	Upper primary school (5-9. grades)	4 lessons (1-1-1-1-0)	General secondary school	Lower grades (1-4. grades)	4 lessons (1-1-1-1)
General secondary school	(1-4. grades)	3 lessons (1-1-1-0)		Upper grades (5-8. grades)	2 lessons (2-0-0-0)

III. RESULTS

A. The national core curriculum in Slovakia

In Slovakia, performance and content standards are linked to each topic in the IT curriculum. The performance standard is a coherent system that teachers can further detail, refine, and expand with additional test tasks, taking into account the current abilities of their students. The purpose of content standards is not to transfer ready-made knowledge but to develop skills that help students acquire new knowledge. To this end, students should be given the opportunity to work with concrete objects, observe phenomena, take measurements, and experiment [5].

In Slovakia, the topic of "Safety and Risks" appears four times in the state-issued curriculum: once in lower elementary school, twice in upper elementary school, and once in grammar school [5], [6], [7].

According to the performance standard, by the end of the fourth grade of elementary school, students should be able to discuss the risks of the internet and know the rules for protecting against unauthorised use of email. The content standard states: safe online behaviour [5].

In upper elementary school, the curriculum mentions the topic of safety and risks twice. According to the performance standard, by the end of 6th grade, students should be able to discuss various Internet risks and know how to protect applications and data (including email) against unauthorised access. In addition, students should be able to talk about cybercrime and judge the reliability of information found on the internet. The content standard covers malicious software (e.g., viruses), the authenticity of information obtained, risks on social networking sites, the spread of viruses and spam messages, safe and ethical online behaviour, and the activities of hackers.

By the end of the 8th grade of elementary school, students should be able to discuss the risks of the Internet based on performance standards. They should be able to assess what information needs to be protected from misuse. They should apply rules for secure access to email accounts and social platforms and prevent unauthorised use of computers. In addition, they should recognise the risks posed by malicious software. Discuss cybercrime. Talk about computer crime and the dangers of illegal content, and be able to evaluate the credibility of online information. The content standard at this level discusses viruses as malicious software and spam messages in detail, as well as the use of antivirus programs for virus protection. It also emphasises the importance of password quality as a fundamental element of protection, as well as the issue of the reliability of information obtained in the online space and on social platforms. The processes covered include computer viruses and spam messages, safe and ethical online behaviour, and the activities of hackers [6].

The topics of security and risk play a role in the IT curriculum for grammar school education. According to the performance standard, students must be able to assess the risks of working with malicious software. In addition, they must be familiar with the rules for secure access to e-mails, social networking sites, and computers in order to prevent unauthorised use. Students must ensure that data and communications are protected against misuse and be able to assess the reliability of information found on websites. They are

expected to recognise cybercrime and distinguish illegal content. The content standard discusses in detail the spread of computer viruses and spam messages, the principles of safe and ethical behaviour on the Internet, the activities of hackers, and how to avoid disclosing personal information online [7].

B. The national core curriculum in Austria

In Austria, there is no separate IT education at the primary school level; it is integrated into other subjects, such as German, German as a second language, mathematics, art, technology, and design, where students can encounter IT skills. The framework curriculum defines certain competencies that students must have by the end of primary school. Students must therefore know how to use information technologies safely and responsibly. They must understand and be able to follow simple instructions and create new works. They must learn how to use digital tools and the internet in their learning. They must be able to create and design digital drawings and images. Another competency goal is to experience self-efficacy through the creative and diverse use of digital technologies [8].

The digital literacy curriculum developed for students in grades 1–4 of lower secondary education aims to equip students with age-appropriate skills for handling digital information, collaborating and communicating, and acting safely and responsibly in the digital environment. The curriculum integrates both computer science and media literacy, with a particular emphasis on child protection and managing the risks of the digital environment.

In Grade 1, students are able to perform simple internet searches using the basic functions of search engines and evaluate the quality of the information found based on basic criteria. They understand how personal data can be used and are able to take basic precautions to protect their data. Digital technologies enable new forms of collaboration; students learn to collaborate with others online in a respectful and responsible manner. Areas of application include the collection, storage, and use of user data.

In Grade 2, students describe how information is provided and retrieved, and how data is transmitted over the Internet. They are able to identify, explain, and apply licensing models, particularly open-source systems, including Creative Commons licences and open educational resources.

In Grade 3, students analyse changes in media usage habits and reflect on the possibilities and risks of personalised media usage. They become aware of the compromises associated with digital technologies that affect their daily activities and future career opportunities. In the area of responsible information and data management, students understand the conditions, advantages, and disadvantages of personalised search routines and are able to conduct targeted, independent information searches, using appropriate sources and critically evaluating the information they find. In the area of communication and collaboration, students understand how cloud-based systems work, taking into account critical factors such as server location, data security, and data protection, and recognise the trade-offs between disclosure and confidentiality of information. They consciously plan their digital identity and monitor or protect their reputation. Areas of application include the use of encryption methods for secure information transfer, secure password use and two-factor authentication, physical and digital protection of electronic information, and dealing with real-world cybersecurity issues such as cyberbullying, cyber grooming, and identity theft. Students are able to take appropriate precautions to protect their devices and content from viruses and malware.

In Grade 4, students reflect on the possibilities and limitations of artificial intelligence and practice performing data backups and restores. They understand the risks of collecting, analysing, and linking user data, including negligence, misuse, and surveillance, and act responsibly in this area. In media-related competencies, students understand the mechanisms of media reality construction, the collection and analysis of information and data, and the process of image, sound, and data manipulation. They communicate responsibly in digital media and exchange data while respecting copyright and the right to one's own image. Areas of application include the phenomenon of viral content and related courses of action, as well as knowledge and application of data protection legal bases (e.g., GDPR).

At the upper level of secondary school education, based on the national core curriculum for computer science, students should be able to understand and apply measures and legal principles related to data security, data protection, and copyright [9].

IV. DISCUSSION

Based on the analyzed curriculum requirements, it can be concluded that Slovakia and Austria approach information security education with different emphases and structures, but both countries recognize the growing importance of the topic. In Slovakia, information security is introduced at an early age: by the end of lower elementary school, students are taught about the dangers of the internet and the basic rules for protecting themselves against unauthorized use of email. This suggests that the Slovak education system builds information security knowledge in accordance with the principle of gradualism, adapted to age-specific characteristics.

In Slovakia in upper elementary school and, in Austria, in lower secondary school, the curricula of both countries prescribe more in-depth content, such as secure password use, assessing the credibility of information, and protection against malicious programs. At the same time, the Austrian framework curriculum takes a more detailed approach at this stage, with a greater emphasis on cyberbullying, cyber grooming, identity theft, and the management and protection of user data. This level of detail suggests that Austria is consciously responding to the new risks of the information society.

It is worth highlighting the element of the Austrian curriculum that requires reflection on the possibilities and limitations of artificial intelligence, as well as practice in data backup and recovery. In addition, there is a strong emphasis on developing media literacy, including understanding the construction of media reality, recognizing data and media manipulation, and discussing various licenses and the GDPR in detail. These elements show that the Austrian curriculum integrates new technological and social challenges more effectively, especially in the areas of data protection and artificial intelligence.

At the secondary school level, however, there is a marked difference between the two countries. While Austria uses relatively general terms at this level with regard to data security, data protection, and copyright, Slovakia sets out detailed, competency- and content-orientated requirements. These include recognizing the risks of malicious software, protecting email and social media accounts, identifying cybercrime, and distinguishing illegal content. Slovak content standards refer to specific phenomena such as viruses, spam, hacker activity, and personal data protection, which enhances their practical applicability.

V. CONCLUSION

This study compared the appearance of information security in the state-issued IT framework plans of Slovakia and Austria. Based on the research, it can be said that the structure of the education systems in the two countries differs significantly: while in Slovakia, primary school lasts 9 years and secondary school lasts 4 years, in Austria, primary school lasts 4 years and secondary school lasts 8 years. In Austria, based on the state-issued curriculum, students only encounter IT education within the framework of digital literacy at the lower level of secondary school. In Slovakia, IT education begins in the third grade of primary school. As students are starting to use various devices (phones, laptops) at an increasingly early age and are encountering the dangers of the internet sooner and sooner, it is particularly important that they learn as early as possible the coping strategies they can use in the event of a potential danger.

Overall, Slovakia consistently and comprehensively incorporates information security into the curricula for each age group, while Austria provides faster and more comprehensive responses to newer threats, particularly artificial intelligence and data protection. The strengths of the two approaches complement each other: the Slovak model offers depth and specificity, while the Austrian framework curriculum has advantages in terms of topicality and the integration of modern technological challenges.

REFERENCES

- [1] D. Mandić and G. Kiss, "Password usage in Hungary and Slovakia among users of smart devices," *Biztonságtudományi Szemle*, vol. 6, no. 2, 2024.
- [2] D. Smahel, H. Machackova, G. Mascheroni, L. Dedkova, E. Staksrud, K. Ólafsson, S. Livingstone, and U. Hasebrink, *EU Kids Online 2020: Survey Results from 19 Countries*. London, U.K.: EU Kids Online, 2020. [Online]. Available: <https://doi.org/10.21953/lse.47fdeqj01ofo>
- [3] OECD, *How's Life for Children in the Digital Age?* Paris, France: OECD Publishing, 2025. [Online]. Available: <https://doi.org/10.1787/0854b900-en>

- [4] F. Quayyum, D. S. Cruzes, and L. Jaccheri, "Cybersecurity awareness for children" *International Journal of Child-Computer Interaction*, vol. 30, Dec. 2021. [Online]. Available: <https://doi.org/10.1016/j.ijcci.2021.100343>
- [5] Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky, *Informatika – primárne vzdelávanie*, Feb. 9, 2022. [Online]. Available: <https://www.minedu.sk/data/att/542/22036.5e0a91.pdf>. [Accessed: Oct. 26, 2025].
- [6] Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky, *Informatika – nižšie stredné vzdelávanie*, Feb. 9, 2022. [Online]. Available: <https://www.minedu.sk/data/att/2d2/22091.7fd543.pdf>. [Accessed: Oct. 25, 2025].
- [7] Národný inštitút vzdelávania a mládeže, *Informatika – gymnázium so štvorročným a päťročným vzdelávacím programom*, [Online]. Available: https://www.statpedu.sk/files/articles/dokumenty/inovovany-statny-vzdelavaci-program/informatika_g_4_5_r.pdf. [Accessed: Oct. 27, 2025].
- [8] Rechtsinformationssystem des Bundes (RIS), Bundeskanzleramt der Republik Österreich, Bundesrecht konsolidiert: Lehrplan der Volksschule, Anl. 1, tagesaktuelle Fassung, BGBl. Nr. 134/1963, zuletzt geändert durch BGBl. II Nr. 178/2025. [Online]. Available: <https://www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10009275&Anlage=1>. [Accessed: Jan. 20, 2026].
- [9] Rechtsinformationssystem des Bundes (RIS), Bundeskanzleramt der Republik Österreich, Bundesrecht konsolidiert: Lehrpläne – allgemeinbildende höhere Schulen, Anl. 1, tagesaktuelle Fassung, BGBl. Nr. 88/1985, zuletzt geändert durch BGBl. II Nr. 204/2024. [Online]. Available: <https://www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10008568&Anlage=1>. [Accessed: Jan. 19, 2026].
- [10] B. Pásztor, "Az információbiztonság megjelenése a szlovákiai és a lengyelországi államilag kiadott kerettantervben," *Gradus*, vol. 11, no. 3, 2024. [Online]. Available: <https://doi.org/10.47833/2024.3.CSC.004>
- [11] Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky, 2015. [Online]. Available: <https://www.minedu.sk/data/att/473/22021.94bec0.pdf>. [Accessed: Oct. 29, 2025].
- [12] Národný inštitút vzdelávania a mládeže, 2015. [Online]. Available: https://www.statpedu.sk/files/articles/dokumenty/inovovany-statny-vzdelavaci-program/rup_g_4_r_s_vyuc_jaz_slov.pdf. [Accessed: Oct. 26, 2025].