Issues and challenges of creating a safe digital learning environment for students: focusing on privacy, personal data, and student data protection

Hyeon-Seon Jeong

(Professor, Gyeongin National University of Education,

Director of Media Literacy Research Center)

1. Overview of AI Digital Textbook Development Policy Promotion

□ Background and timeline of the AI digital textbook development policy

○ In the "AI Digital Textbook Promotion Plan (Draft)" (June 2023), the Ministry of Education stated that "personalized education to develop each student into a human resource is not easy in the classroom environment," and that "advanced technologies such as AI, which have been developing at a rapid pace in recent years, have created the conditions for digital technology to

realize personalized education that takes into account students' capabilities and characteristics."

- In this regard, it is important to consider the changing role of teachers, the plan wrote, "Teachers need to understand each student's learning path and knowledge level to design data-driven, engaging lessons, personalize instruction, and record growth so that students can have more 'success experiences' through learning."

○ The AI digital textbooks will be introduced in Math, English, information (Technology), and Korean (for learners with special education needs) subjects from 2025 in accordance with the 2022 Revised Curriculum, and will be expanded to subjects such as Korean, Social Studies, Science, Technology & Home by 2028.

- Excludes grades 1-2 and subjects that build aesthetic sensitivity, social and emotional skills, and character (Ethics, Music, Art, Physical Education) to account for student development.

□ AI Digital Textbook: Concept and Core Services

○ AI digital textbooks are defined as "textbooks equipped with various learning materials and learning support functions using information technology, including artificial intelligence, to support various customized learning

opportunities according to students' individual abilities and levels."

- Key features include learning diagnostics and analytics powered by AI, personalized learning that reflects an individual's learning level and pace, and learning courseware designed from the student's perspective.

○ Key services that should be included in an AI digital textbook include

- Students: Diagnose and analyze learning, recommend the best path and content for each student
- Teachers: Data-driven learning management, including lesson design and personalized prescription support (AI assistant), reorganization and addition of content, and student learning history
- Students, Teachers and Parents): Provide students with learning data analysis via dashboards, enable communication between education stakeholders (teachers, students, and parents), unified login, easy and convenient UI/UX configuration, and ensure accessibility (Universal Design for Learning [UDL], multilingual support, etc.)

○ Therefore, 'AI digital textbook' is not a 'textbook' centered on learning materials as the general public has experienced so far, but a 'data-based learning management system' that uses digital technology to collect and utilize a wide range of data about students for learning diagnosis and analysis,

lesson design, and personalized prescription support.

<Figure 1> AI digital textbook vision diagram

Source: Ministry of Education, Korea Institute of Education and Research Information, "Guidelines for the Development of AI Digital Textbooks," 2023.8.

□ Who develops and operates AI digital textbooks

○ Regarding the development and operation of digital textbooks, the Ministry of

Education decided to provide cloud (SaaS) based web services through cross-ministerial cooperation (NIA: National Information Agency) rather than the existing ePub service method, as "private publishers develop digital textbooks that apply AI technology according to the characteristics of each course and directly provide infrastructure operation and customer service as a service provider."

- The data of teachers and students collected through AI digital textbooks should be used for the purpose of AI digital textbook services and not for their own services, and it is proposed to separate and manage the infrastructure of AI digital textbooks from the infrastructure of their own services, but there is no specific guideline, regulation, reporting, punishment rules, and discussion of management and supervisory bodies.

□ Concerns in developing AI digital textbooks

○ The Department of Education refers to the UNCRC General Comment No. 25 and has included in its policy announcements that when developing policies, programs, and training on children's rights in relation to the digital environment, States parties should involve all children and give due weight to their views.

- However, the only specifics regarding this are that it must "utilize user experience analysis and design thinking tools by referring to the National Design Team Manual in accordance with the public participation provisions of Article 52 of the Administrative Procedure Act, and reflect the needs of students, parents, and teachers as users in the development process."

• The UN Convention on the Rights of the Child defines "child" as any infant, child, or adolescent up to the age of 18.

○ The application of children's rights in digital environments as outlined in the UNCRC General Comment No. 25 to the development of AI digital textbooks is not just about designing for user needs and ease of use. The rights of the child in the digital environment include not only the right to access to the opportunities that digital technologies can provide, but also the right to be protected from the risks and negative impacts of using digital technologies.

- Therefore, from the perspective of children's rights in the digital environment, the development and use of AI digital textbooks must address the following issues: is the data-driven learning that is intended to be provided through AI and digital technologies desirable for the overall development and learning of students; at what level and in what ways is the application of AI and digital technologies and the

collection and use of learning data for this purpose appropriate for the cognitive, emotional, and social development and well-being of children and adolescents; and the scope of student data that may be collected in the course of using AI digital textbooks, when and how consent will be obtained from students and parents for the type, form, storage, use, and disposal, and for how long and how it will be disposed of; and how students and parents who do not consent to the use of AI digital textbooks or who want very limited access due to concerns about the various "risks" and negative impacts that AI and digital technologies may have on students can refuse or withdraw their consent, How can their choice to learn in other ways and their right to their data be guaranteed within the public education system; how will the safety of the data collected and the protection of student privacy be overseen, regulated, reported, and punished; how will students' data rights be explained and consent sought in language and visuals that are easy for students and parents to understand; and how will broad input from experts in the field, parents (guardians), and students on these issues be sought and public consultation undertaken. However, to date, there has been no discussion of this at all.

2. Issues related to students' safety in the development and

application of AI digital textbooks and recommendations from the international communities to protect children's rights

□ Lack of child protection measures in accordance with children's rights in digital environments

○ On March 2, 2021, the UN Committee on the Rights of the Child released its General Comment No. 25, "Children's rights in the digital environment" (hereinafter General Comment) (UNICEF Korea, 2021), which provides comprehensive yet specific recommendations on how the existing UN Convention on the Rights of the Child (the Convention) should be understood and implemented in a digital environment.

- General Comments are guidelines for the interpretation and application of an international treaty or plan of action by different countries and have the status of international law.

- The Government of the Republic of Korea is a State party to the Convention, having acceded to the United Nations on September 17, 1991, and ratified the Convention on December 20 of the same year, and is therefore obliged to respect the rights of children in the digital environment as set out in the General Comment and to take

steps to ensure their implementation.

○ The General Comment notes that the digital environment is playing an increasingly important role in children's lives as societal functions, including education, administrative services, and commercial services, are rapidly becoming dependent on digital technologies, and calls for appropriate action by States parties to the Convention.

- Whereas the digital environment offers new opportunities to ensure that children's rights are realized, it also creates new opportunities for children to be treated unfairly or discriminated against, including by being excluded from digital technologies and services, exposed to hate speech in the course of using digital technologies, and exposed to other discrimination and risks that may arise from automated processes that filter, collect, and make decisions based on data that is biased or value-biased against children, and States Parties to the Convention should take proactive measures to protect children from such discrimination and risks.
- It also recommends that countries should provide training and advice to parents, guardians, educators and others on the proper use of digital devices, based on the latest research on the impact of digital technology on brain plasticity during early childhood and adolescence, when critical neurological processes are rapidly developing.

○ The General Comment emphasizes the importance of ensuring children's right to privacy in digital environments because it is essential to their agency, dignity, safety, and the exercise of their rights.

- Recognizing that children's privacy may be threatened by the collection and processing of information by public authorities, businesses, and other entities in digital environments where children's personal information is used to provide education, health, and other benefits, and by criminal activity such as identity theft, we recommend that digital technologies used by children should be designed in accordance with the principle of minimizing the collection of personal information to comply with the best interests of the child.

- Personal information collected, distributed, and used in the digital environment includes information about a child's identity, activities (including learning), location, communication, emotions, health, and social relationships, and may be combined with biometric data to accurately identify a specific child.

- Whereas, in an environment where the use of artificial intelligence and big data technologies is becoming increasingly widespread as a result of the development of related industries, digital practices such as automation of information processing, data collection, behavioral tracking, mandatory identification, information filtering, and public surveillance are becoming commonplace, and whereas such practices

may arbitrarily and unlawfully violate children's right to privacy, which may have adverse consequences that affect children's lives not only temporarily, but also on an ongoing basis in the future, and whereas the State has a duty to regulate and monitor companies to protect children from such violations of privacy

○ The report also recommends that States must respect children's views when developing legislation, policies, programs, services, and education to create a digital environment for children; create ways for children's views to be heard; and ensure that digital service providers create appropriate safeguards for children and actively engage children and take their views into account when developing products and services, with appropriate safeguards in place.

<Table 1> UNCRC General Comment No. 25 'E. The Right to Privacy'

67. privacy is essential to children's agency, dignity, safety, and the exercise of their rights. Children's personal information is used to provide education, health, and other benefits. However, a child's privacy can be threatened by the collection and processing of information by public authorities, businesses, and other organizations, or by criminal activity such as identity theft. Threats to privacy can come from children themselves, family members and friends who post photos of children online, and others with whom they share their information.

68. A child's personal information includes information about the child's identity, activities, location, communications, emotions, health, and relationships. A child can also be accurately identified by a combination of certain personal data, such as biometric data. Digital practices such as automated processing, data collection, behavioral targeting, mandatory identification, information filtering, and mass surveillance are becoming commonplace. These practices can arbitrarily and unlawfully violate a child's right to privacy. They can also have a lasting impact on a child's life later in life, leading to negative consequences for the child.

Interference in a child's private life is only permissible if it is not arbitrary or unlawful. Therefore, such interference must be authorized by law, have a legitimate purpose, follow the principle of minimizing the collection of personal data, be proportionate and designed to comply with the best interests of the child. It must also not be incompatible with the provisions, purposes, and objectives of the Convention on the Rights of the Child.

70. States parties should take legislative, administrative and other measures to respect and protect children's privacy in all organizations and settings that process children's information. Legislation should include strong data safeguards, transparency of data processing, independent oversight, and access to remedies. States Parties should ensure that privacy-by-design is applied

to digital products and services that affect children. States Parties should regularly review their privacy and data protection legislation and ensure that their information processing procedures and practices prevent intentional invasion of privacy or accidental disclosure of children's information. Where encryption is considered an appropriate means, States Parties should consider appropriate measures to detect and report child sexual exploitation and abuse or sexual abuse material. These measures should be strictly limited in accordance with the principles of lawfulness, necessity, and proportionality.

71. Where consent is sought to process children's data, States Parties should ensure that the child (and sometimes the parent or guardian, taking into account the child's age and evolving capacities) is informed of the content and is comfortable deciding whether to give consent, and this must take place before the data is processed. Where the processing of a child's personal data requires the consent of a parent or guardian and the child's consent is insufficient, States Parties should ensure that the entity processing such data has properly communicated the consent to the parent or guardian and that the consent is meaningful and has been given by the child's parent or guardian.

72. States Parties should ensure that children and their parents or guardians can easily access their stored information under reasonable and lawful conditions, correct inaccurate or outdated information, and delete information that is unlawfully or unnecessarily held by public authorities, individuals or other entities. States Parties should also ensure that children have the right to withdraw their consent and object to the processing of their personal data if the data controller overrides the basis for processing and fails to prove its lawfulness. States Parties should also provide children, parents, and guardians with information about this in child-friendly languages

and accessible formats.

73. ensure that children's personal information is processed in compliance with lawful procedures, including periodic audits and accountability measures, and is accessible only to designated authorities, organizations, and individuals. Children's information collected for a specific purpose, including digital criminal records, must be protected and be of an exclusive nature, i.e., used only for that purpose, and must not be unlawfully or unnecessarily retained or used for any other purpose. Where information collected in one context legitimately benefits a child when provided in another context, such as schooling and higher education, it should be used in an accountable and transparent manner and based on the consent of the child, parent, or guardian.

74. Laws and measures to protect privacy and information should not arbitrarily restrict freedom of expression or the right to protection. States parties should ensure that information protection laws respect children's privacy and personal data in relation to the digital environment. With the constant innovation of technology, the digital environment continues to expand and now encompasses services and goods such as clothing and toys. As the environments in which children spend time become "connected" to each other through sensors embedded in automated systems, States Parties should ensure that products and services in digital environments are subject to high standards of information and other privacy protections. These "connected environments" include streets, schools, libraries sports venues, entertainment venues, commercial and public facilities including shops and movie theaters, and homes.

75. All surveillance of digital records, including automated processing of personal data, must respect the child's right to privacy and must not occur routinely and indiscriminately or without the

child's (or, in the case of very young children, their parent or guardian's) knowledge. Commercial, educational, and care settings should allow people to opt out of surveillance if they do not wish to do so, and should consider means of minimizing interference with their privacy while still achieving the given purpose of the surveillance.

The digital environment poses several challenges for parents and guardians to respect children's right to privacy. Technologies that monitor children's online activities for safety, such as tracking the devices and services they use, can, if not used carefully, prevent children from accessing helplines or searching for sensitive information. States Parties should inform children, parents and guardians, and the public about the importance of children's right to privacy and what behaviors threaten this right. They should also inform children about ways to respect and protect their privacy while keeping them safe in the digital environment. The level of monitoring by parents and guardians of children's digital activities should be adapted to take into account children's evolving abilities.

77. Many children use avatars or pseudonyms to protect their identity online, which is important for their privacy. However, as such anonymity can be used as a routine means of concealing harmful or illegal behavior, such as cyber-attacks, hate speech, sexual exploitation and abuse, States Parties should require an integrated approach of safety-by-design and privacy-by-design to protect privacy while ensuring that anonymity does not become a negative tool. Protecting children's privacy in digital environments is especially important in situations where the presence of a parent or guardian poses a threat to the child's safety or where conflicts arise regarding the child's care. In these cases, additional interventions may be needed, such as family counseling or other services, to protect the child's right to privacy.

78. Providers of prevention or counseling services in the digital environment should be exempt from the requirement of parental consent for children to use their services. When children use these services, a high level of protection of children and their privacy must be maintained.

Source: UNICEF Korea Committee, UNCRC General Comment No. 25, Children's rights in the digital environment, March 2021.

□ Privacy and Cloud Security Issues in AI Digital Textbook Development Guidelines

○ The "Guidelines for the Development of AI Digital Textbooks" (Aug. 2023), presented by the Ministry of Education and the Korean Institute of Education and Research Information, refer to the 10 detailed principles of the "Ethical Principles of Artificial Intelligence in Education" (Ministry of Education, 2022), including "Ensure the safety of educational parties" (⑧), "Ensure transparency and accountability of data processing" (⑨), and "Rationally utilize data and protect privacy" (⑩).

- However, there are no specific guidelines for applying these ethical principles to the development of AI digital textbooks, and no suggestions for supervision and regulation by national authorities.

○ The Ministry of Science and ICT will support the development of AI digital textbooks by the Ministry of Education through the K-Cloud project.

- The K-Cloud project is a project to enhance the competitiveness of the domestic

cloud industry by building and operating ultra-high-speed and low-power data centers based on domestic AI semiconductors, and ultimately provide AI services on the cloud, and AI digital textbooks are one of these AI services (Ministry of Science and ICT, Internet Promotion Division, March 24, 2023).

- The purpose of the K-Cloud Project Education SaaS Development Support Project is to "support the development of educational software (cloud) to provide various innovative educational services by incorporating advanced technologies such as artificial intelligence." Targeting domestic educational software (cloud) development companies (digital textbook publishers can participate by forming a consortium with technology companies), a total of 3.7 billion won was provided for "development costs such as design, implementation, and testing of cloud-based educational services, software development tools in conjunction with cloud companies, technical training and consulting support, business costs for sales of developed services, and sales support."

- Considering the nature of the K-Cloud project and the "Edtech Promotion Plan" announced by the Ministry of Education (September 18, 2023), the policy to develop AI digital textbooks can be seen as having a strong purpose of fostering the edtech industry.

○ According to the AI Digital Textbook Development Guidelines (Ministry of

Education, Korea Institute of Education and Research Information, 2023: 47), AI digital textbooks developed based on cloud services utilize students' academic information, and student learning data is linked to the learning data hub built by the government, so information protection and security certification are important.

- K-Cloud developers shall give priority to cloud computing services that have received security certification pursuant to Articles 20, 23, and 23-2 of the Cloud Computing Act and Article 15-6 of the Enforcement Decree of the Act, and shall comply with the standards (including administrative, physical, and technical protection measures) regarding the quality, performance, and information protection of cloud computing services in order to secure the reliability of cloud computing services and protect users.
- As a mandatory compliance, developers are required to use infrastructure (IaaS) and SW (SaaS) with a security certification of "medium" or higher, and to submit a security certificate or proof that they have applied for a security certification when submitting their audit to verify security certification.
- The key item that distinguishes "medium" from "high" security certification is technical protection measures. In order to obtain a "High" security certification, a company must "provide cloud computing services in the public business network

area that handles important information such as national institutions, etc." and "provide security management measures corresponding to the internal network and corresponding cloud services so that there is no connection with the external Internet," and "automate periodic (one month) checks on whether updates are required to keep the security patches of information assets related to the provision of cloud services up to date. As the information on the AI digital textbook platform can be clearly verified after development, it is necessary to determine the cloud security certification level based on the information.

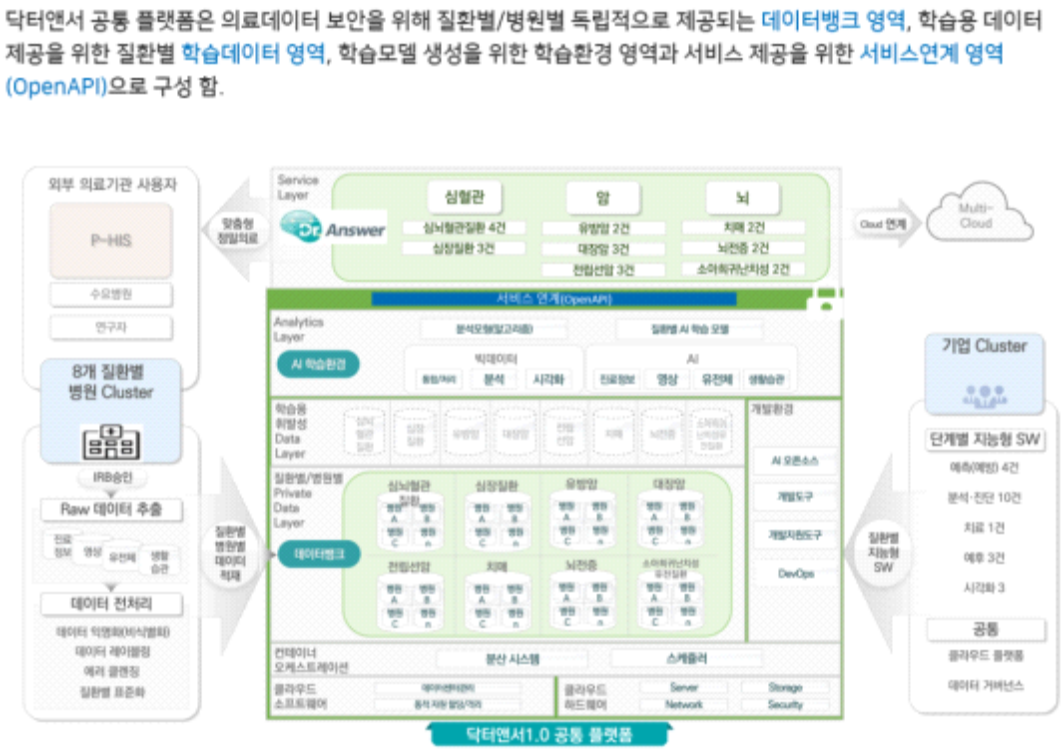
<Figure 2> Security authentication types

등급	시스템 등급 분류	평가기준
하	개인정보 미포함, 공개된 공공 데이터 운영 시스템	· 합리화: 물리적 망분리 → 논리적 망분리 - 국내 서비스형 소프트웨어(SaaS) 사업자가 공공시장에 신규 진입할 수 있도록 기존의 민간·공공 영역 간 물리적 분리 요건 완화 - 단 클라우드 시스템과 데이터의 물리적 위치는 국내한정
중	비공개 업무자료를 포함 또는 운영하는 시스템 중요도에 따라 행정내부업무 시스템도 포함 가능	· 현행 수준 유지 - 보안성을 담보한 네트워크 접근 허용 · 합리적 간소화 - 기존유형(IaaS, SaaS 표준, SaaS 간편) 통폐합 및 불필요 항목 삭제 - 이용 기관별 테이블 분리 기준 완화
상	민감정보 포함, 행정 내부업무 운영 시스템	· 보안 강화

Source: Korea Finance Intelligence Service, "Trends in the Reorganization of Cloud Service Security Certification System (CSAP)," April 24, 2023.

- In the healthcare sector, security models are being independently researched, and the national project 'Doctor & Sur' (Seonyeon, July 31, 2020) is also following a high level of license compliance (Korea Internet & Security Agency, 2020). In the education sector, specific discussions on what data should be allowed to be collected and utilized are urgently needed, and further research and action is needed on what level of security model should be applied depending on the sensitivity of the data collected.

<Figure 3> 'Dr. Answer' 1.0 Common Platform



Source: Sun-soo Yeon, "21 kinds of SW-intensive medical devices 'Dr.&Seo', spurring licensing", TECHWORLD, 2020.7.31.

□ Concerns about the collection and use of student sensitive information in AI digital textbooks

○ AI textbooks are composed of publicly provided AI textbook portal services and privately provided subject-specific AI textbook services.

○ Services for students, teachers, and parents include "Utilizing AI technology to provide analysis results by diagnosing individual students' strengths and weaknesses, learning attitudes, and understanding," "Comprehensively analyzing students' learning patterns (interests, preferences, etc.) and levels to recommend content suitable for learners," "Analyzing learning patterns and activities to provide additional learning elements, Q&A, etc.", "Organize personalized services by collecting and analyzing learners' learning activity status and learning data", "Provide learning management functions for teachers such as learners' learning situation and academic emotions", and "Provide a way to systematically accumulate and manage learning data for each student".

<Figure 4> AI Digital Textbook Service Configuration

Source: Ministry of Education, Korea Institute of Education and Research Information, "Guidelines for the Development of AI Digital Textbooks," 2023.8.

○ The information included in the AI digital textbook service, especially the analysis of "learning attitudes," "interests, preferences," "learning activity status," and "learning mood," is sensitive information that is classified as high-risk under the EU Artificial Intelligence Act, as it operates an AI system to infer human emotions in an educational environment.

- The lack of public awareness of the privacy and security issues of AI digital textbooks, which may contain sensitive information about students, and the lack of in-depth

discussions among policy authorities is very concerning in terms of children's privacy and personal information.

○ Given that edtech is part of the digital environment that greatly affects children's information and privacy, it is necessary to conduct in-depth research and review by experts to protect children from harm; to fully explain to the public, including students, parents, and teachers, the issues related to privacy and security of AI digital textbook development; and to ensure sufficient time for public deliberation and the establishment of legislative, supervisory, and regulatory bodies, personnel, and budgets to create a safe educational environment.

- The rapid pace at which AI digital textbooks are being developed in the absence of public discussion of these issues is extremely concerning in terms of the risks to children in the digital environment.

○ The EU Artificial Intelligence Directive categorizes AI systems used in education as "high-risk" and has very specific compliance requirements for high-risk AI.

- In light of this, the development and application of AI digital textbooks must be preceded by in-depth social deliberation and measures such as legislative and regulatory oversight to protect students' rights, including their right to privacy,

personal data, and data protection as set forth in the UNCRC General Comment No. 25.

□ See: EU "Artificial Intelligence Act" (Council of the European Union, 2024.1.26.)

○ The EU Artificial Intelligence Directive categorizes AI systems used in education as high-risk. "High-risk AI systems" in education include AI systems used to make admissions or admission decisions or to allocate people to education or training institutions, and AI systems used for the purpose of assessing learning outcomes or assessing the appropriate level of education that an individual receives or could receive (Kempf, 2024. 2.13.).

○ AI systems intended to be used to monitor and catch students cheating on tests may also qualify as high-risk AI systems. Lawmakers determined that it is appropriate for these systems to be considered high-risk because they "can determine an individual's educational and professional path and affect their ability to earn a living."

○ It also warns that, if improperly designed and used, these systems "can be intrusive, in particular by inappropriately entering and interfering with a person's privacy or space, violating the right to education and training and the

right to non-discrimination, and perpetuating patterns of discrimination that have historically existed against women, people of certain ages, people with disabilities, people of certain racial or ethnic origin, and people of certain sexual orientations" (Kempf, 2024.2.13.).

○ The EU Artificial Intelligence Directive categorizes biometric AI systems as high-risk, with stricter restrictions on the use of AI systems that infer human emotions in educational settings.

<Table 2> 'Compliance requirements for high-risk AI systems' in Article 9 of the EU Artificial Intelligence Directive

 Risk Management System

- Establish, implement, document, review, and update risk management systems for the entire lifecycle.

- Identify and analyze risks to health, safety, and fundamental rights

- Estimating and assessing the risk of foreseeable misuse conditions

- Eliminate or reduce technically identified risks through proper design and development

- Implement appropriate mitigation and control measures to address risks that cannot be eliminated.

- Testing for the purpose of identifying targeted risk management actions

 Data and governance

- Apply proper data governance and management practices

- Data preparation processing tasks such as annotation, labeling, cleaning, updating, enrichment, and aggregation

- Formulate assumptions about what the data should measure and represent

- Evaluate the availability, quantity, and appropriateness of the data sets you need

- Investigations that consider bias that could negatively impact health, safety, and fundamental rights

- Identification of data gaps or deficiencies and how to resolve them

 Technical Documentation

- Written before the system goes to market and kept up to date

- Demonstrate compliance with legal requirements and clarify information needed to assess compliance

 Archiving

- Automatically log events ("logs") for the life of the system

□ Transparency and information about distributors

- Provide concise, complete, accurate, and clear information that is accessible and understandable to users

- Identity and contact information of the service provider and (if applicable) its authorized representatives

- Characteristics, capabilities, and performance limitations of high-risk AI systems

- Changes to high-risk AI systems and performance

□ human supervision

- Design and develop AI systems in a way that allows for effective human oversight while they are in use.

Source: Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts: Analysis of the final compromise text with a view to agreement*, 2024.1.26. 2024(116~118).

3. international community guidelines for digital service providers to ensure the rights and safety of children (students)

□ "OECD Guidelines for Digital Service Providers" (OECD, 2021)

○ The OECD adopted the 2021 Recommendation on Children in Digital Environments, calling for the best interests of children to be prioritized and for age-appropriate child safety measures to be incorporated into the design of digital services.

- Additional guidance in 2021 states that digital service providers should take a "proactive approach" to ensuring children's rights and safety, "including a safety by design approach to addressing risks."

○ The OECD's guidelines on children's privacy and data protection are as follows

<Table 3> OECD Guidelines for Digital Service Providers

If you provide digital services that are directed to children or reasonably foreseeable to be accessed or used by children and collect, process, share, and use personal data, digital service providers must

- Provide children and their parents, guardians, and caregivers with information about how their personal data is collected, disclosed, provided, or otherwise used in language that is concise, understandable, accessible, clear, and explained in an age-appropriate manner.
- Limit the collection of personal data and its subsequent use or disclosure to third parties in order to fulfill the provision of services in the best interests of the child.
- We do not use children's data in ways that we have evidence are harmful to the welfare of children.
- Do not allow profiling or automated decision-making of children, including on eLearning platforms, unless there is a compelling reason to do so and appropriate measures are in place to protect children from harm.

Source: OECD, *OECD Guidelines for Digital Service Providers*, 2021.

□ "Unicef Manifesto for Improving Children's Data Governance" (Unicef, 2021)

○ UNICEF released a declaration in 2021 that aims to encourage governments and companies to address children's rights in their data governance frameworks.

- This includes 10 principles to prevent the misuse of children's data and violations of children's rights under the UN Convention on the Rights of the Child.

<Table 4> UNICEF Manifesto for Improving Child Data Governance

The 10 Principles of the UNICEF Manifesto
The international community should consider the following actions when developing and implementing data governance frameworks. 1. protect children and their rights through child-centered data governance. Such data governance should adhere to internationally agreed standards that minimize the use of surveillance and algorithms to profile children's behavior. 2. prioritize the best interests of the child in all decisions regarding the child's data. Governments and businesses should prioritize children's rights in their data collection, processing, and storage practices. 3. consider children's unique identities, changing capabilities, and circumstances in your data governance framework. Data governance rules should be flexible because children are all different and mature with age. Marginalized children should never be left behind. 4. Shift responsibility for data protection from children to businesses and governments. Extend protections to all children under 18, regardless of age of consent. 5. work with children and communities in the policymaking and management of their data. Through a decentralized data governance model, children and communities should have more say in how their data is processed, with whom it is processed, and with whom it is shared. 6. represent the interests of children within administrative and judicial proceedings and remedy

mechanisms. It is essential to integrate children's rights into existing mechanisms, such as the work of data protection authorities.

7. provide adequate resources to implement child-inclusive data governance frameworks. Data protection authorities and technology companies should hire staff who understand children's rights, and governments should allocate funding for regulatory oversight.
8. Leverage policy innovation in data governance to solve complex problems and accelerate outcomes for children. Policy innovation can help public authorities make the most of data while protecting children's rights.
9. Knowledge gaps in the area of data governance for children need to be addressed. There are several pressing knowledge gaps that require further research to ensure that data governance regulations are evidence-based.
10. strengthen international cooperation for child data governance and facilitate knowledge and policy transfer between countries. The Declaration calls for increased international coordination on laws and policies. Lack of harmonization of data governance laws at the national level can lead to jurisdictional claims and conflicts.

Source: UNICEF, *The Case for Better Governance of Children's Data: A Manifesto,* 2021.5.

□ World Privacy Congress Resolution on the Digital Rights of the Child (October 2021)

○ A meeting of data protection authorities held in October 2021 under the auspices of the Global Privacy Congress unanimously adopted a resolution submitted by CNIL of France and Garante of Italy and co-sponsored by 21 authorities from around the world.

- The resolution reiterates the key elements of the UNCRC's General Comment No. 25, calling on States to

  • Prohibits manipulating a child or influencing a child's behavior in a way that may be contrary to the child's best interests.

  • Prohibits the use or transfer of children's data to third parties for commercial or advertising purposes, and the use of marketing techniques to induce children to provide personal data.

○ The resolution states that online service providers should integrate the promotion of children's best interests and respect for children's rights into the design of their services.

- According to the resolution, online service providers should integrate the promotion of children's best interests and respect for children's rights into the design of their services; tracking should be turned off by default; tracking should not be done through the system itself without the child's knowledge; age verification

mechanisms should work to ensure that they are proportionate to the risk and protect privacy; and service providers should not profile children based on digital records of their actual or inferred characteristics for commercial purposes.

<Table 5> World Privacy Congress resolution on children's digital rights

Online service providers should integrate the promotion of children's best interests and respect for children's rights into the design of their services, including by providing privacy impact assessments, child rights impact assessments, data encryption solutions, understandable and easy-to-use privacy settings, preferences that maximize the protection of children's personal data, in particular the ability to disable certain options by default, such as geolocation and profiling, and consulting with children, parents, or child advocates during the development of their services.

Source: Global Privacy Assembly, *43rd Closed Session of the Global Privacy Assembly: Adopted Resolution on Children's Digital Rights*, 2021.10.

□ 5Rights Foundation's "International Comparative Study on Child Data Protection" (Oct. 2022)

○ The 5Rights Foundation, a non-profit organization that works closely with the United Nations to advocate for children's rights in the digital environment, has published "International Comparative Study on Child Data Protection"

(October 2022), which compares the child protection resolutions of various international organizations, including the UNCRC General Comment No. 25, as well as the main contents and implications of child data protection regimes and related laws and policies in various countries, including the United Kingdom, the Netherlands, Ireland, France, Sweden, California, Australia, India, Brazil, and New Zealand.

- The Age Appropriate Design Code (AADC): a code of practice for online services (Information Commissioner's Office, 2022), published by the UK Information Commissioner's Office, became law in 2020 and has been in force since 2021. Its key findings can be used to inform detailed guidelines or testing criteria for the development of AI digital textbooks and suggest the need for legislation, policy, funding, and staffing to ensure that AI digital textbooks are regularly subjected to data protection impact assessments by independent research organizations.

<Table 6> UK "Code for Designing Online Services Appropriate to the Age of Users"

15 Standards for Age-Appropriate Design Code

1. Best interests of the child: When designing and developing online services that are likely to be accessed by children, the best interests of the child must be a primary consideration.
2. Data Protection Impact Assessment: Services must conduct a Data Protection Impact Assessment to assess and mitigate the risks to children's rights and freedoms arising from the processing of data by that service.
3. Enforce age appropriateness: Services should take a risk-based approach to recognizing the age of individual users. Age should be set with a level of certainty appropriate to the risk, or the criteria should be applied to all users.
4. Transparency: Privacy information provided to users and other posted terms, policies, and community standards must be concise, conspicuous, and written in clear language appropriate to the age of the child.
5. Harmful Use of Data: The Service shall not use a child's personal data in a manner that is harmful to the child's welfare or contrary to industry practices, other regulatory provisions, or governmental recommendations.
6. Policies and Community Standards: The Service must comply with its own published terms, policies, and community standards.
7. Default settings: Settings should be set to "High Privacy" by default, unless there is a good reason to change the default setting based on your child's best interests.
8. Data minimization: Only collect and retain the minimum personal data necessary to provide elements of the service in which the child is actively and knowingly engaged.
9. Data Sharing: Children's data should not be disclosed unless there is a compelling reason to do so,

taking into account the child's best interests.

10. Geolocation: The Geolocation option should be off by default.

11. Parental Controls: Services must provide age-appropriate information about their parental controls. If the service allows parents or guardians to monitor their child's online activity or track their child's location, the service must clearly inform children that they are being monitored.

12. Profiling: The Profiling option should be set to "Off" by default. Profiling is only allowed when appropriate measures are in place to protect children from harmful effects.

13. Nudging Techniques: You may not use nudging techniques to induce or encourage children to provide unnecessary personal data or to weaken or disable privacy protections.

*Nudge technique: A subtle design strategy that gently nudges a user's behavior to facilitate a desired decision or action.

14. Connected toys and devices: Connected toys or devices must include effective tools to ensure compliance with the Code.

*Connected Toy: A smart toy that is connected via the internet or other network technology to provide a variety of interactions and features. They can be connected to online services via Wi-Fi, Bluetooth, and other connectivity methods to provide features such as updateable content, voice recognition, remote control, and learning algorithms, but they can also pose privacy and security concerns, including privacy, data security, and child safety, and should be used with caution.

15. Online tools: Services should provide prominent and accessible tools for children to exercise their data protection rights and report concerns

Source: Information Commissioner's Office, *Age Appropriate Design: A code of practice for online services*, 2022.10.17.

4. Urgent challenges to creating a safe learning environment for students

☐ Specific legislative, policy, and regulatory measures to protect student privacy and personal information

○ Regarding the development of AI digital textbooks, it is necessary to urgently supplement the guidelines for the development of AI digital textbooks by specifically and clearly classifying and defining the data of minors that can be collected and utilized in AI digital textbooks and the sensitive data and information that should not be collected and utilized, and to establish and enforce specific and effective laws and regulations to protect the personal information and privacy of children (students), and to establish and enforce management supervision and regulatory mechanisms for developers (publishers).

- For data protection and private information regulations to protect students' personal information and privacy, we analyze the relevant provisions of the Elementary and Secondary Education Act, which applies to minors as well as the Data 3 Act, which applies to adults; the UN Convention on the Rights of the Child's General Comment No. 25; the OECD Guidelines for Digital Service Providers; and the UNICEF Declaration on Improving Children's Data Governance, The World Privacy Congress Resolution on the Digital Rights of the Child, the 5Rights Foundation's "International Comparative Study on Children's Data Protection," and the UK Information Commissioner's "Code for the Design of Age-Appropriate Online Services," among other international recommendations and laws.
- Korea needs to lead the way in ensuring that AI digital textbook developers develop technology that meets regional standards such as those in the U.S., EU, and elsewhere, with the highest level of child protection measures appropriate to Korea's national character, and urgently needs research studies, public hearings with students, parents, teachers, and the general public, and funding and manpower to do so.

○ The Elementary and Secondary Education Act states that student information may not be used without the consent of the school principal, student, or parent.

<Table 7> Article 30.6 of the Elementary and Secondary Education Act

(Restrictions on the provision of student-related materials)

(1) The principal of a school shall not provide school life records pursuant to Article 25 and medical examination records pursuant to Article 7(3) of the School Health Act to a third party without the consent of the student (or, if the student is a minor, the student and the student's parent or guardian). However, this shall not apply in any of the following cases.

1. necessary for an administrative agency with oversight and audit authority over the school to fulfill its responsibilities
2. provide school records pursuant to Article 25 for use in the selection of students for admission to a postsecondary school
3. for purposes such as statistical compilations and academic research, in a form that does not identify the author of the data.
4. as necessary for the investigation and prosecution of crimes and the establishment and maintenance of legal proceedings
5. as necessary for the court to conduct its judicial business
6. as otherwise provided by applicable law

② When providing data to a third party pursuant to Paragraph 1, the head of the school may restrict the purpose, method of use, and other necessary matters to the recipient of the data or request the recipient to take necessary measures to ensure the safety of the data.

(③) The person receiving the materials pursuant to paragraph (1) shall not use the materials for any purpose other than the purpose for which the materials were received.

[Revised March 21, 2012].

Source: Elementary and Secondary Education Act [Enacted 2023.9.27.] [Act No. 19738, partially amended 2023.9.27.]

○ Utilizing student data and AI technology in education requires the same level of governance and security as in finance and healthcare.

○ It is necessary for the Ministry of Education and the Ministry of Science, ICT, and Future Planning to work together to jointly prepare policies for such research, legislation, and administrative oversight, and for an independent agency to have the manpower and budget to implement the policies.

□ AI Digital Textbook's cloud CSAP security certification needs to be upgraded to the 'Top' level

○ Currently, the AI Digital Textbook's cloud security certification is at the 'Medium' level, but it needs to be upgraded to 'High'.

- According to the Ministry of Education's guidelines for developing AI digital textbooks, the learning data collected during the process of utilizing AI digital textbooks is processed according to the purpose and transmitted to the learning data hub through the dataset created.

- The types of datasets sent include country-level learning datasets, integrated dashboard datasets, learning history datasets, and datasets for AI training.

  • Country-level learning datasets: datasets for analyzing learning at the country, state, and school level

  • Unified Dashboard Dataset: Dataset for configuring the Unified Dashboard in the AI Digital Textbook Portal

  • Learning history datasets: Datasets sent in response to data subject (student teacher, parent) data transfer requests.

  • Dataset for AI training: A dataset to collect learning data from each developer and provide it as future AI training data to develop AI digital textbook services such as

AI-based learning analysis.

- Requires (simulation-based) impact assessment and safeguards for what remains of these datasets as log data.

□ Many of the AI courseware and platforms being used in education have woefully inadequate privacy policies and practices and guidance for students and parents, raising alarms and prompting regulatory action.

○ There are currently a number of generative AI-based edtech platforms on the market and in use, and the protection of student personal information and privacy and security measures of these edtech platforms require full investigation and continuous monitoring and disclosure of information in accordance with the "Safety Survey," "Publication and Disclosure of In-depth Analysis of Harm Information," "Consumer Harm Monitoring System," "Damage Remedy Counseling," "Dispute Mediation," and "Consumer Information" implemented by the Ministry of Consumer Affairs.

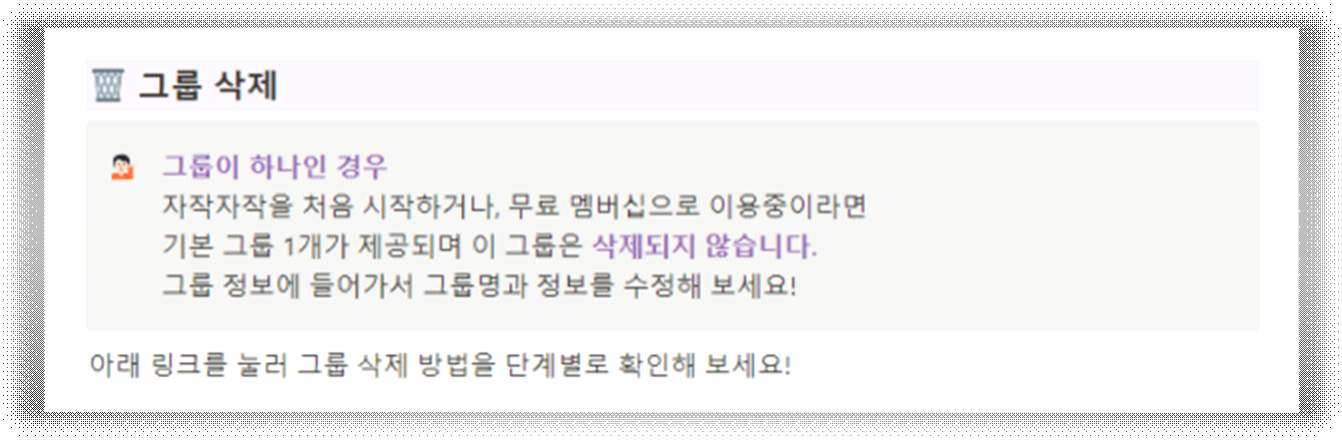
<Figure 4> Consumer Safety Services in Consumer Resources

Source: Consumer Resources homepage (https://www.kca.go.kr/home/main.do#Page2)

○ Among the generative AI-based writing feedback services that are widely used in schools, J-service has a major problem in terms of student safety and protection, as when teachers disclose the code of their class groups for training purposes, all personal and sensitive information such as names, assignments, and grades of students in the group are disclosed to the outside world.

- Free users of J-services can only use one group (class), and when using only one group, it is not possible to delete the group, which makes it difficult to delete the contents.

<Figure 5> Group deletion notice for digital service J program using generative AI

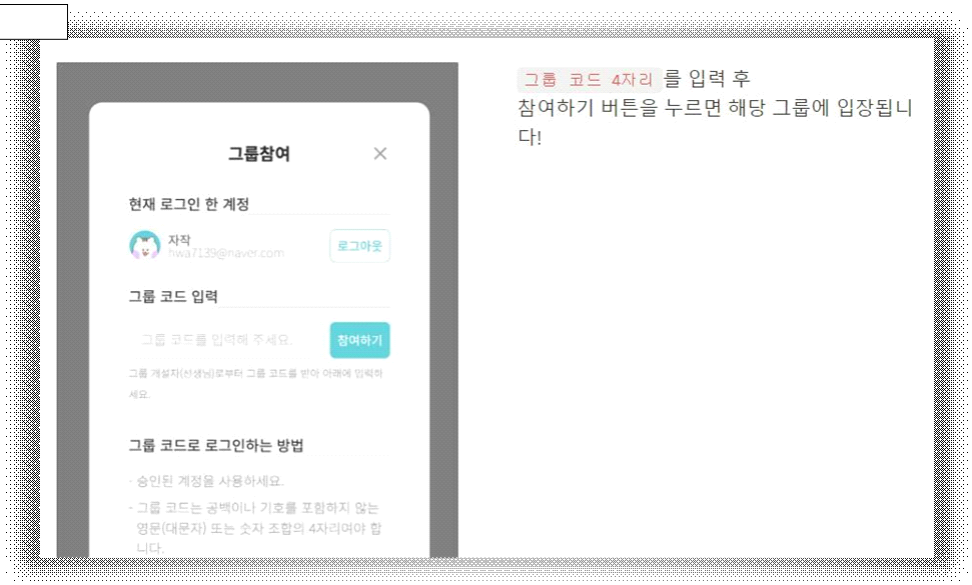


Resource: J Programming Guide (Last accessed: 2024.2.21.)

https://teampl100.notion.site/e770c748c8314586aaa416f97ed4c80e?pvs=25

- This service does not require a teacher (group administrator) to 'accept entry' when entering a 'group (class)', so anyone can immediately join the group without verifying their identity by entering the 4-digit group code. As a result, outsiders who are not related to the group can easily join the group and view the personal information of existing members (students), such as their names and email addresses, as well as the learning outputs uploaded by students without any sanctions, and thus have access to sensitive information that may be contained in students' work.

<Figure 6> Group participation notice in the J program

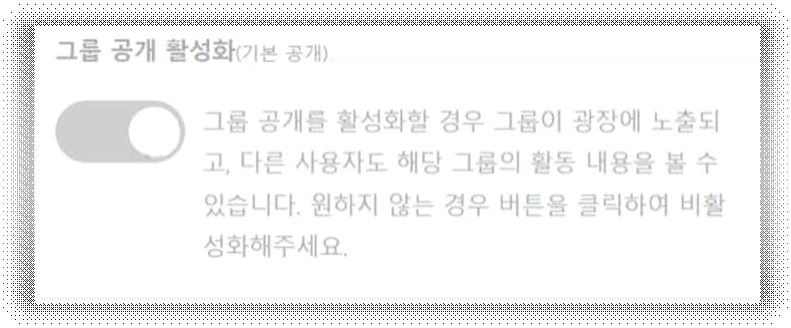


Resource: J Programming Guide (Last accessed: 2024.2.21.)

https://te ampl100.notion.site/e770c748c8314586aaa416f97ed4c80e?pvs=25

- The service also makes it easy for people outside of your school to view your group's activity by enabling "group visibility".

<Figure 7> Enabling group visibility (default visibility) in J Program



Resource: Guide to Using the J Program (last accessed 2024.2.21.)

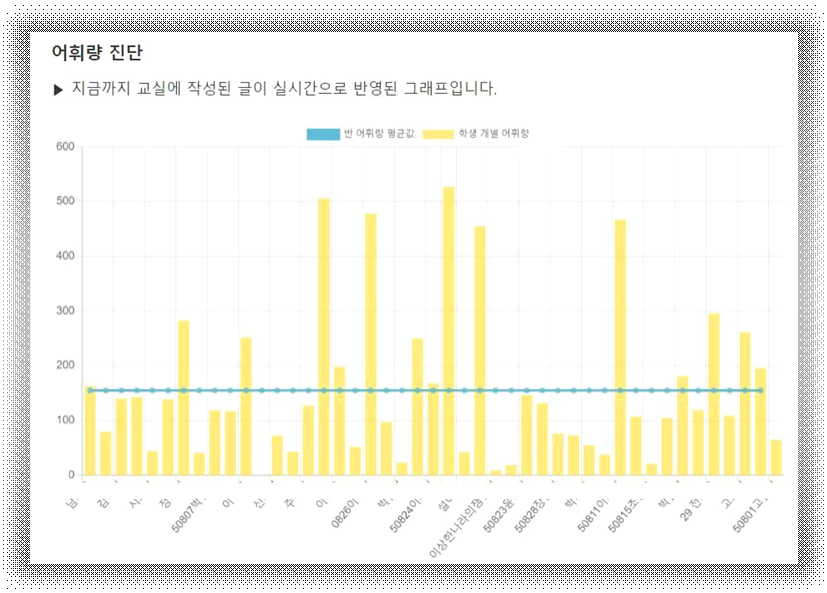
https://t eampl100.notion.site/e770c748c8314586aaa416f97ed4c80e?pvs=25

- However, despite these various issues, there are no regulations, entities, personnel,

and budgets in place to oversee and regulate edtech services, leaving students' personal, private, and sensitive information at significant risk.

- On the other hand, these services provide learning data such as vocabulary diagnosis for students, as shown in <Figure 8> below, but it is difficult to judge how these data are calculated and how they can be used to diagnose individual students' learning, and it is difficult to evaluate the quality of the service because there is no independent and professional research on the effectiveness of educational use.

<Figure 8> Training data provided by the J program (vocabulary diagnosis)



Resource: J Programming Guide (Last accessed: 2024.2.21.)

https://t[redacted]eampl100.notion.site/e770c748c8314586aaa416f97ed4c80e?pvs=25

5. conclude

□ Need for Expert Review and Public Hearing on AI Digital Textbook Adoption and Development Guidelines

○ The name "textbook" may mislead students, parents, teachers, and the general public into thinking that it is a digitized learning resource, so a friendly and transparent explanation is needed to make it easy and clear to understand that it actually has the nature and function of an "educational platform.

○ Current AI digital curricula can be problematic in that they force teachers and students to rely too heavily on AI and digital technologies to deliver lessons and assessments that rely on data-datable learning outcomes.

○ Student use of AI technologies and digital technologies should be student and teacher choice, taking into account student development, learning goals and objectives, and the nature of the learning content, and should respect parents' values and choices about child rearing and education, recognizing that the use of digital technologies extends beyond school and into the home.

○ Development guidelines need to be supplemented to ensure that not all lessons rely on the use of digital devices and technology, and to suggest alternative activities, such as in-person activities.

○ Development guidelines need to be supplemented to ensure that AI and

digital technologies are selected appropriately and balanced in lessons based on the learning context, goals, content, and form of the activity, including face-to-face interaction in the classroom space and handwriting, face-to-face listening and conversation, and analog methods that utilize the body, tangible objects, and printed learning materials and activities, as well as the use of digital materials and tools and LMSs that are not accompanied by AI technologies.

○ When using wi-fi in schools, a large number of simultaneous connections can lead to slow or inaccessible AI and internet access, and digital devices used by students can often break, malfunction, or be damaged, so it's important to design core learning materials and activities to be easy to print so that learning can continue even under these circumstances.

○ The policy materials and reports on AI digital textbooks published by the Ministry of Education and the Korean Institute of Education and Research Information emphasize the benefits of AI and digital technology utilization and data-driven learning one-sidedly, and it is necessary to ensure diversity to ensure balanced education based on the latest research findings.

□ Precautions to protect students from the dangers of AI and digital technology are woefully inadequate and urgently needed.

○ UN Committee on the Rights of the Child, General Comment No. 25, Children's rights and information rights in the digital environment and the need to work towards quality textbooks that support healthy and happy development.

○ The content of student-created work products may reveal personal and other sensitive information, including students' names and personal relationships. Therefore, when storing students' learning outcomes as data, it is necessary to apply safety-by-design and privacy-by-design to ensure that only the necessary parts of the learning outcomes are stored as data, and to study specific measures to supplement the development guidelines.

○ The guidelines for the development of AI digital textbooks need to be supplemented to respect the information human rights of students, parents, and teachers, prioritize safety, including the protection of students' personal information and privacy, and incorporate the practice of digital citizenship into teaching, learning, and assessment, and reflect this in the testing criteria.

○ Learning outcomes in a variety of subjects, including Korean, Social Studies, and English, may include photos, videos, and texts that may contain student

voices, facial expressions, and distinctive gestures, and may be personally identifiable. As a result, safety regulations and design must be strengthened to ensure that these artifacts are not stored on platforms and used as datasets by AI technologies, and that regulations on how and for how long artifacts are stored and disposed of, as well as student and parental consent and withdrawal processes are easily explained and implemented in plain language.

○ Article 10 of the Basic Law for the Promotion of Digital-Based Remote Education (abbreviated as the Remote Education Act, enacted March 25, 2022 [Act No. 18459, enacted September 24, 2021]), Article 54 of the Basic Law on Digital Media Literacy Education and Intelligence Informatization, which mandates access to, utilization of, understanding of, and critical ability in digital media and prevention of over-reliance on information and communication media and devices, and Article 54 of the Basic Law on Digital Media Literacy Education and Intelligence Informatization, requires that practical education and digital citizenship education to prevent improper use of devices and appropriate education on device management and security management for students be reflected in the operation of school curriculum organization at each grade level.

<Table 8> Article 10 of the Basic Act on the Revitalization of Digital-based Remote Education

(such as teaching digital media literacy) (1) In order to enable students to participate in distance education on their own initiative, the head of a school or other institution shall provide digital media literacy education, including the following items 1. improve access to and utilization of digital media 2. improve understanding and critical skills of digital media 3. Increase social engagement through digital media 4. enhance democratic communication through digital media The state and local governments may provide preventive education in accordance with Article 54 of the Basic Law on Information and Communication to prevent students from becoming physically and mentally overly dependent on information and communication media or information and communication devices.

○ The use of eye-tracking technology in the learning of young students is likely to cause significant stress and anxiety for the learners and could be considered emotional child abuse. While technologies that require biometric information from students, including eye-tracking technology, are valuable as tools for

academic research, in the real world of learning and teaching, they can be used for excessive surveillance of students and jeopardize their privacy and mental health, and biometric information is considered high-risk sensitive information. Therefore, the use of these technologies needs to be very carefully considered based on academic research and expert opinion.

References

MSIT Press Release, "MSIT and Ministry of Education Actively Cooperate to Develop Artificial Intelligence (AI) Digital Textbooks - Developing AI Digital Textbooks by Publishers through the Korean Internet-based Resource Sharing Project (K-Cloud Project)," March 24, 2023.

Ministry of Education Press Release, 「AI Digital Textbook Promotion Plan (Draft), 2023.6.

Ministry of Education & Korea Education and Research Information Services, "Guidelines for the Development of AI Digital Textbooks," August 2023.

Sun Soo-yeon, "21 kinds of SW-intensive medical devices, 'Dr. Answer', spurring

licensing", 『TECHWORLD』, 2020.7.31. (Last retrieved on 2024.2.20.) <https://www.epnc.co.kr/news/articleView.html?idxno=101153>

UNICEF Korea, Committee on the Rights of the Child General Comment No. 25: Children's rights in the digital environment, 2021. (Last accessed: 2024.2.20.) <https://www.unicef.or.kr/what-we-do/database/page/14#tagBox>

Korea Internet & Security Agency, Digital Healthcare Security Model (Summary), 2020.12.

Korea Finance Intelligence Service, Trends in the Reorganization of Cloud Service Security Assurance Program (CSAP), 2023.4.24. (Last retrieved 2024.2.20.) <https://www.fis.kr/ko/major_biz/cyber_safety_oper/attack_info/notice_issue?articleSeq=3504>

Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts: Analysis of the final compromise text with a view to agreement*, 2024.1.26. (Last retrieved 2024.2.20.) <https://artificialintelligenceact.eu/the-act/>

5Rights Foundation, *Approaches to Children's Data Protection: A comparative international mapping*, 2022.8. (last visited 2024.2.20.), <https://5rightsfoundation.com/Approaches-to-Childrens-Data-Protection---.pdf>

Global Privacy Assembly, *43rd Closed Session of the Global Privacy Assembly: Adopted Resolution on Children's Digital Rights*, 2021.10. (Last accessed: 2024.2.20.) <https://globalprivacyassembly.org/wp-content/uploads/2021/10/20211025-GPA-Resolution-Childrens-Digital-Rights-Final-Adopted.pdf>

Information Commissioner's Office, U.K., *Age Appropriate Design: A code of practice for online services*, 2022.10.17. (Last accessed:2024.2.20.) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/>

Kempt, A-L., "A Guide to High-Risk AI System under the EU AI Act", Pinsent Masons, 2024.2.13. (last accessed 2024.2.20.) <https://www.pinsentmasons.com/out-law/guides/guide-to-high-risk-ai-systems-under-the-eu-ai-act>

OECD, *OECD Guidelines for Digital Service Providers*, 2021. (Last accessed:2024.2.20.)
<https://www.oecd.org/mcm/OECD%20Guidelines%20for%20Digital%20Service%20Providers.pdf>

UNICEF, *The Case for Better Governance of Children's Data: A Manifesto*, May 2021 (last visited 2024.2.20.)
<https://www.unicef.org/globalinsight/reports/better-governance-childrens-data-manifesto>