48th Closed Session of the Global Privacy Assembly

November 2026

Resolution on Artificial Intelligence (AI) in Education

This Resolution is submitted by the Digital Education Working Group Drafting Team on AI in Education.

SPONSORS:

- Catalan Data Protection Authority, Catalonia
- Commission for Personal Data Protection, Bulgaria
- Commission Nationale de l'Informatique et des Libertés, France
- Estonian Data Protection Inspectorate, Estonia
- Information Commission's Office, United Kingdom
- Office of the Information and Privacy Commissioner, Ontario, Canada
- Office of the Privacy Commissioner for Personal Data, Hong Kong, China

CO-SPONSORS:

- Office of the Privacy Commissioner, Canada
- Agency for Access to Public Information, Argentina
- State Commissioner for Data Protection and Freedom of Information, Rhineland-Palatinate, Germany
- Privacy Protection Authority, Israel
- Information and Data Protection Commissioner's Office of Albania
- Belgian Data Protection Authority
- Data Protection Agency, Croatia
- National Commission for the control and the protection of personal data (CNDP), Morocco

The 48th Global Privacy Assembly 2026:

Acknowledging the transformative nature of Artificial Intelligence (AI) for education, and the rapid pace of adoption by teachers and students[1] around the globe;

Recalling that data protection laws and privacy principles apply to AI technologies, even as different jurisdictions continue to develop AI specific laws and policies;

Recognising that a key role for data protection authorities is protecting children's data and privacy, because children are vulnerable and their personal data is inherently sensitive;

Recognising that AI tools involving large-scale collection, use, and disclosure of personal data across the whole AI lifecycle should be safe and robust, including from development and training through to subsequent deployment;

Recognising that the content of interactions with an AI system[2] reflects the children's level of knowledge and competence in a given field, as well as—where applicable—their thought processes, judgement, and critical thinking, and that these constitute personal data, requiring Educational AI tools[3] to be transparent about the information they are collecting and using;

Acknowledging that children may derive benefits from artificial intelligence tools (AI tools) developed for educational uses ("educational AI"[4]), through:

- Distance learning;
- Adaptive tutoring for focused skills;
- Responses to individual learning challenges;
- increased access to information and translation;
- real time feedback.

Acknowledging that children may also face significant privacy risks from educational AI use, including:

- unnecessary and disproportionate collection and storage of personal data, including for commercial purposes without appropriate safeguards,
- restricted choice regarding secondary uses for that information, including for AI training or improvement, sharing with third parties, or other commercial uses,
- profiling, inferences and categorisations that might impact or even pre-emptively shape their educational path,

---

[1] This resolution refers to children, understood as individuals under the age of 18, in the first two stages of formal education.

[2] "AI system" means a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that may influence physical or virtual environments – OECD Recommendation of the Council on Artificial Intelligence : https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449

[3] "AI tool" is used throughout to refer broadly to applications of artificial intelligence and Generative AI in educational settings, including platforms, applications, services, and technologies

[4] "educational AI" refers to the integration of artificial intelligence and advanced technologies into learning environments.

- manipulative design including engagement-maximising features, or the collection of information to facilitate more effective means to influence children as a target audience,
- inaccurate information, AI hallucinations, standardised/generic content and data recycling
- regulatory gaps in the legal guardrails required to ensure children's best interests sit at the heart of educational technologies; and
- data breaches, which pose significant risks, as personal data may be misused for malicious purposes (e.g. cybercrime).

Acknowledging that AI use may impact the wider education ecosystem by:

- promoting an overly standardised approach to teaching and assessment;
- normalising the use of commercial digital technologies by children and the sharing of personal data relating to teaching methods and educational outcomes outside the educational sphere;
- exacerbating inequalities in access to and use of an AI system. Not all pupils have access to the same knowledge or have the same digital tools available at home.

Recalling that the fundamental right to privacy and the protection of personal data implies a high degree of individual choice, control and agency over the collection, use and disclosure of personal data;

Acknowledging that children are rights holders who deserve informational self-determination including meaningful opportunities to question the educational technologies they use and the ways in which these technologies use their personal data, commensurate with their developmental stage and in keeping with their rights to autonomy and dignity;

Highlighting that research with children clearly demonstrates that they have a range of concerns about the ways AI impacts their personal data, their education, including a loss of critical thinking due to cognitive offloading, and their lives and that it is important not only to listen to children's voices but also to take their views into account, in accordance with Article 12 of the United Nations Convention on the Rights of the Child (UNCRC);

Recalling the widespread and growing international recognition of the significant risks to younger generations growing up in a digital environment where AI is increasingly integrated, and the need to put in place strong and age-appropriate privacy safeguards to protect children and youth in education settings, reflected in relevant international sources and GPA resolutions and documents, detailed in Annex 1;

Acknowledging that general purpose AI tools, and more broadly, educational technologies, operate in an environment where public/private partnerships or procurements are the norm, which introduces the risk of data commercialisation interests diverging from public education goals;

Affirming that governments bear responsibility for ensuring that children's best interests, including their data protection and privacy, are considered when educational AI is assessed and authorised;

Emphasising that children deserve special protection in educational contexts, and the critical role educational institutions play in a child's life, with recognition of:

- Their status as distinct rights holders under the Convention on the Rights of the Child.

- The compulsory nature of attending an educational institution for many years, for most children;
- The special role of educational institutions as trusted, safe, caring, and developmentally appropriate spaces for children's learning and emotional growth, including the opportunities to make mistakes, explore ideas, and change over time;
- The potential impact of inappropriate data collection, use, or disclosure in school settings on a child's social and emotional well-being and life chances; and
- The important role education plays in the development of digital literacy as a foundational component of contemporary life. This implies that future generations should develop AI and data literacy and be prepared to understand the limitations and risks of AI tools, use them responsibly and critically, and protect themselves against potential harm arising from their use.

Understanding that children's needs and capacities change rapidly and significantly as they progress through their formal education, and that these evolving needs and capacities should be taken into consideration when making decisions about whether, when, and how AI tools and technologies are introduced to their learning environments, ensuring such decisions are always centred on the best interests of the child;

Affirming that good data governance in relation to AI technologies and tools in educational settings is a foundational safeguard for children's privacy, security, equality, autonomy and dignity;

Asserting that all AI tools approved for use in educational settings must be valid and reliable, safe, privacy protective, human rights affirming, transparent, and accountable. AI tools should be assessed for their suitability in educational settings and should be proven to support pedagogical objectives while minimising privacy and safety risks for children;

Asserting that privacy and safety should be a precondition for AI procurement and use in educational settings, and that the principles of necessity and proportionality for personal data use must be met in every case of AI system processing;

Acknowledging the critical importance of safeguarding the sensitive personal data of vulnerable children, and not retaining their information any longer than necessary, to mitigate the risk of data breaches that could potentially present life-long privacy risks, permanently compromising their present and future safety;

Recognising that children, as the primary rights holders affected by the use of AI in education, and their legal guardians should receive age-appropriate information, training and guidance to develop their own critical skills in relation to AI use. Support and meaningful opportunities to ask questions, challenge outcomes, seek human involvement and exercise their rights should also be provided. Where possible, they should be meaningfully involved in conversations about policy and decisions that impact them in using AI tools in education;

Recognising that many actors are involved in the design, development, procurement, deployment, oversight and use of educational AI tools throughout the AI lifecycle, and have distinct responsibilities in upholding children's fundamental rights, protecting their personal data, and supporting safe, fair and developmentally appropriate learning environments. These actors include:

- **Edtech providers and AI developers**, including subcontractors and sub processors, should ensure that educational AI tools are designed and deployed in accordance with children's rights, applicable data protection and privacy laws and requirements in their respective jurisdictions, as well as applicable global or regional frameworks. This includes transparency about the categories and purposes of personal data being processed, including whether data is used to train or improve AI systems, and having appropriate safeguards in place to support lawfulness, fairness, accuracy, data minimisation, purpose limitation, security and data subject rights**.**
- **Legislators, education ministries, local authorities and other public bodies** that are responsible for passing laws and setting education policy or mandating AI tools should ensure their instruments and decisions comply with international best practices, data protection and privacy requirements.
- **Education providing institutions** including schools, early years settings bodies, that procure, approve or use educational AI tools should determine the purposes and means of processing of personal data and should comply with their obligations as controllers, including in relation to lawfulness, transparency, data minimisation, security, accountability and children's rights. They should also assess whether each educational AI tool is appropriate for its intended purpose and, where identified risks or compliance issues cannot be adequately mitigated, refrain from using it.
- **Teachers and other education professionals** should use educational AI tools consistently with applicable data protection and privacy requirements. Where they may lack the technical knowledge needed to understand the privacy and data protection risks associated with such tools, including free or non-approved AI tools, they should be provided with appropriate support and guidance, including dedicated training and information.
- **Data protection and privacy authorities**, in accordance with their respective mandates, should provide guidance to relevant stakeholders, promote compliance with data protection and privacy laws, and support education and public awareness about the risks and safeguards associated with AI in education. They should also enforce data protection standards through regular audits and sanctions, when necessary.

Recognising that the rights to data protection and privacy are fundamental, yet are in tension with the way many AI technologies are designed, trained, implemented and maintained. We assert the importance of the following key data protection principles, which should be followed by all actors throughout the AI lifecycle (including design, development, selection, procurement, deployment, oversight and use of AI tools in education) in accordance with local data protection and privacy laws:

1. Best interests of the child as a primary consideration

- The best interests of the child must be a primary consideration for all actors throughout the lifecycle of an educational AI tool. No commercial interest, operational convenience or efficiency gain may override this principle. A child-rights-based approach is necessary to protect children from potential AI-related harms.

- When the use of AI tools is mandated by the school, for compulsory use by the students, all actors involved need to ensure that the tool is safe and child rights-respecting.

- In assessing the best interests of a child, responsible actors should make every effort to balance and reconcile a child's right to privacy protection with other rights and interests that can be affected by processing their personal data, including the right to non-discrimination, the right to education, and the right to be heard.

2. Roles and responsibilities

- All actors throughout the lifecycle of an educational AI tool must define their responsibilities and, if necessary, those of other parties involved in the processing of children's personal data (controller, joint controllers, processor/contractor or sub processor/subcontractor). Compliance by one actor does not release any other actor from their own responsibilities.

- All actors that design and develop AI tools for educational purposes must comply with data protection requirements.

- To support efficient compliance with data protection obligations, the person designated with privacy responsibilities (such as a Data Protection Officer) should be involved from the earliest stage of the decision to develop or use an AI tool.

3. Legal basis and strict limitation of purpose

- Each actor that processes personal data must identify and rely on a legal basis for each processing activity, depending on jurisdictional law(s).

- In the educational context, consent may often not be applicable due either to the existence of a power imbalance between the parties involved or because of restrictions in the applicable law, for example, when the legal basis is the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

- If consent is the legal basis for data processing, it must be freely given, specific, informed and unambiguous. Information provided to children or their legal guardians should be clear and readily understandable, taking into account the child's age and capacity. Where legal guardian consent is required or appropriate under the applicable legal framework, its role should be considered in light of the child's age, development stage and evolving capacities, and should not displace the child's own rights and participation to the extent provided by applicable law.

- Children or their legal guardians should not face any negative consequences if they refuse to consent. In case of negative consequences, alternative options with similar effects and consequences must be provided to children and their legal guardians.

- If legitimate interests are the legal basis for data processing, then the best interests, rights and freedoms of children must be appropriately balanced against the business interests of the entity providing the AI service and processing should only take place if the balance favours the child's best interests. In this context, the processing should only take place where the legitimate interests pursued by the controller are not overridden by the interests or

fundamental rights and freedoms of the child, taking particular account of the fact that the data subject is a child; otherwise, such processing should not be carried out.

- Children's data collected or inferred through educational AI tools must not be used for commercial or advertising purposes. Where there is an appropriate legal basis according to jurisdictional law(s) and a defined educational purpose, product improvement or AI model training should only be used for the benefit of, and in the best interests of the children.

- Additional or optional AI features not directly related to the educational function or not demonstrated to be safe, privacy-preserving, and educationally beneficial should not be activated in educational settings.

4. Privacy impact/risk assessments

- Privacy impact/risk assessments may be mandatory and are always best practice for all educational AI tools, before deployment and when products are updated.

- Assessments and, where applicable, mitigation measures undertaken should be documented and made available upon request to supervisory authorities. If necessary, certain parts of the assessment should be made available to teachers and other individuals concerned.

- Assessments require every actor involved in the design and development of the AI tool to provide all necessary information (for example, characteristics, capabilities and limitations of performance of the AI tool). This applies across the entire AI supply chain, including the use, adaptation, integration, updating and monitoring of AI systems.

- Assessments for AI tools require periodic review as circumstances change and should take a risk-based approach that considers not only the risks to privacy and data protection rights, but also the effects on other fundamental rights and interests, that may result from data processing, and which could lead to actual or potential damage/harm (physical, material or non-material damage). This includes the potential for processing to give rise to discrimination, loss of confidentiality of personal data, unauthorised reversal of pseudonymisation or anonymisation, or any other significant disadvantage; or where children might be deprived of their rights and freedoms or prevented from exercising control over their personal data.

5. Privacy by design and default

- All developers and providers of artificial intelligence tools intended for educational use or likely to be used in educational contexts must embed children's rights as a core engineering and governance requirement from the earliest stage of design, to realise the children's best interests, and specifically to:

  (a) apply privacy-by-design principles, including safety by design or age-appropriate design, ensuring that default configurations collect or infer only the minimum data necessary for the educational function, provides for a mechanism to remove any unnecessary data and

that all non-educational features as well as features designed to prolong engagement or further data sharing are disabled by default;

(b) define access controls accurately. It should be clear who may access the data or outputs of any given AI system. This includes clarity regarding teacher, administration, developer access and other parties;

(c) exclude the use of students' data for commercial profiling, advertising, product improvement unrelated to the contracted educational service, and the training of general-purpose commercial artificial intelligence models;

(d) conduct child rights due diligence and bias assessment throughout the development and operation lifecycle, including before deployment and implement mitigation measures to address identified risks where necessary;

(e) implement human oversight architecture ensuring that consequential functions present artificial intelligence outputs as recommendations for human review, not automated determinations;

(f) exclude by design all features incompatible with children's rights, including anthropomorphising[5], sycophancy, subliminal manipulation, social scoring, biometric surveillance and emotion recognition

(g) maintain full transparency about data flows, use of sub processors, accuracy limitations, bias testing results and known risks, and provide this information to deploying organisations before contract signature.

- Unless a specific legal exception applies and additional safeguards are in place, AI tools should not process special category data, such as biometric data, ethnic origin data inferred from names or language, or health data, including data on learning difficulties, or a student's emotional state.

- All actors that use Education AI tools should identify the privacy by design and default features that have been put in place and ensure that they are applied and implemented in an appropriate way, and if necessary incorporate additional safeguards attending the specific context of use.

6. Data Accuracy and Retention Limits

- Children's data processed by AI systems should be accurate. AI-generated assessments or student profiles based on inaccurate data must be correctable.

[5] "AI systems are designed to interact in ways that can appear human, which can lead users towards excessive trust and psychological dependence, but these systems do not process human understanding, experience or social agency": Council of Europe Recommendation CM/Rec(2026)12 of the Committee of Ministers to member States on artificial intelligence literacy (§ III . A. 14)

- Children's data should not be retained any longer than strictly necessary to fulfil each specific educational purpose. Clear retention periods must be defined with attention to children's best interests for every category of student data processed by AI tools.

- Controllers should assure that at the end of the contract/agreement, students' data must be returned to the school and/or effectively deleted by the provider/(sub-)processor.

7. Automated Decision-Making (ADM)

- Decisions likely to impact children should not be based entirely on AI generated outcomes of ADM and should include human involvement, particularly when the ADM may result in negative consequences.

- When using ADM with AI, under lawful conditions, organisations must give prior consideration to the best interests of the children whose personal data is processed, and pursue use of ADM only if it is necessary, proportionate to the educational purpose and does not interfere with child rights including the rights to autonomy, freedom of thought and expression, access to a diversity of information, and development.

- ADM using AI must be transparent and explainable to children and their legal guardians, including providing meaningful information about the logic involved and the significance and envisioned consequences of such processing for individuals.

- There must be a clear and effective way for children or their legal guardians to express their point of view and challenge the ADM.

- Age-appropriate information about the nature of the decision, the systems used, the logic involved, as well as the significance and the envisaged consequences of such processing (the outcome) for the child, should be provided.

- When using ADM, it must be ensured that adequate training for those responsible for overseeing the use of AI tools involving ADM is provided**.** Those responsible for oversight of ADM must be in a position to understand limitations and risks of the system including any biases, the outputs, how such outputs were reached, be capable of identifying errors and alter or reject the AI system's decisions if necessary.

- In any case, AI should support, rather than replace, human decision-making and oversight, with responsible professionals retaining the authority, competence and practical ability to question, override or reject AI-generated outputs.

- AI literacy must be considered as a prerequisite for ensuring that AI systems are aligned with human rights, democracy and the rule of law.

8. Information Security

- Safety and security are essential in AI systems supporting children's educational endeavours. They require robust cyber security protection, provided that such monitoring remains proportionate and does not unnecessarily infringe upon the privacy of children, students and educators.

- Embed Safety and Security by Design principles to proactively anticipate, identify and eliminate online harms before they impact children.
- All actors throughout the lifecycle of an educational AI tool must apply appropriate technical and organisational security measures, proportionate to the risk and the vulnerability of children as data subjects.

9. Transparency and Accountability

- Controllers are accountable for ensuring AI tools comply with privacy and data protection principles and obligations.
- Transparency and explainability are essential. AI systems used in education should be visible, understandable, traceable and explainable, with meaningful disclosure of data uses, human oversight, and include information regarding their functionality in child and youth-friendly language.
- Controllers should inform children or their legal guardians, in age-appropriate language, of matters required under applicable data protection and privacy laws, including:

  (a) The identity and the contact details of the controller and if applicable, the data protection officer;

  (b) The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

  (c) The recipients or categories of recipients of the personal data, if any;

  (d) Where applicable, the fact that the controller and the processors or sub processors intend to transfer personal data to another country or international organisations and the legal basis and transfer tool that applies to the transfer, including any safeguards which need to be put in place;

  (e) The period for which the personal data will be retained and stored, or if that is not possible, the criteria used to determine that period;

  (f) The existence of the rights, when provided for under applicable national law, to request from the controller to access, rectify, erase, or transfer personal data; or to restrict or object to the processing of a child's personal data;

  (g) Clearly set out how rights relating to personal data can be exercised and what controls are available to children and their legal guardians;

  (h) If the right exists in the jurisdiction, the right to lodge a complaint with the relevant supervisory authority;

  (i) A summary of the safety measures implemented (e.g. measures to ensure age-appropriate experiences).

- Children and legal guardians should also be informed about the use of AI in the tool and how it functions. This should include all relevant information to allow them to understand how the

use of an AI tool could affect their rights especially in the context of an educational system, including the risks of possible hallucinations, bias, and manipulative or addictive effects.

- Children, legal guardians, and educators should be clearly informed when educational content, feedback, assessments or other relevant outputs have been generated or materially assisted by AI, through clear labelling or another appropriate form of disclosure.
- Information provided to children or their legal guardians should be easy to access, concise, in language that is clear and readily understandable, taking into account their age and capacity, and delivered in a manner timely to the data processing (just in time information).
- If applicable, children should be informed about the use or processing of their data for training the AI model, product development or other secondary purposes in accordance with applicable laws or guidance, taking into account the best interests of the child and the child's level of maturity.
- If the AI tool incorporates chatbots or an AI assistant, it should notify the person that they are interacting with a machine and not a real person.
- Children and their legal guardians should be informed which of their interactions with an AI system will be visible to their peers, teachers, or others.
- Adaptive learning systems must allow teachers to assess their appropriateness for any given child, and to understand the reasons for outcomes, particularly those consequential to a child's educational path.
- The use of AI tools in education – particularly those used by children with special learning needs and disabilities – must be deployed transparently according to the educational context. Furthermore, the processing of such children's data should not contradict privacy commitments.
- The use of some types of AI-powered plagiarism detection tools by teachers may undermine trust between students and teachers and infringe upon children's rights. Transparency is essential, given the risks of inaccuracy and potential harm resulting from such tools to children, and measures must be put in place to provide protection and/or redress mechanisms appropriate for children and their legal guardians.

10. Data processing agreements and procurement

- The relationship between a controller and a processor should be regulated in a contract or agreement where parties to the contract determine their respective obligations and the instructions necessary for personal data processing in compliance with relevant laws.
- Points to consider include:

  (a) Data protection obligations and instructions for sub processors.

  (b) Information regarding where the data is stored, who has access to it, how long it is retained, and what protections apply to children's interactions with the tool.

(c) Prohibition or authorisation of international data transfers, and where applicable authorisation including requirements and safeguards for overseas hosting, remote access and onward transfers by sub-processors.

(d) Prohibitions on using children's inputs, outputs, chat history, learning analytics or other interaction data to train or improve the provider's AI model except if a legal basis exists, with a clear justification, transparent disclosure, and strong safeguards in the best interests of the child.

(e) Obligations for the processor providing the services requiring written authorisation and a privacy impact/risk assessment for use of AI tools.

(f) Appropriate security measures and access controls.

11. Guarantees of the rights of individuals (children, their legal guardians, and educational professionals)

- Responsible actors must define a clear and agile mechanism to facilitate the effective exercise of privacy and data protection rights in the context of the AI tools. Such mechanisms should also facilitate, where applicable, the effective exercise of other fundamental rights affected by the use of AI in education, including the right to an explanation concerning individual decision-making, non-discrimination and equality, autonomy, and the right to education.
- Children, their legal guardians and education professionals must have accessible and effective mechanisms to question, challenge and report problematic uses or outcomes of AI, with clear routes to human review, correction and remedy. As such, AI literacy should be part of the education process.
- Children and their legal guardians should be provided with accessible, timely and effective mechanisms to contest AI-supported decisions or practices affecting the child and to obtain meaningful human review, correction, redress and other appropriate remedies where harm or infringement of rights has occurred.

The 48th Global Privacy Assembly therefore resolves to:

1. Inform and raise awareness of the privacy and data protection risks and responsibilities of using AI in educational settings, which includes but is not limited to the considerations set out in this resolution.

2. Encourage members' use of this Resolution to develop additional guidelines that assist educational authorities and AI systems providers and developers in meeting their data protection and privacy obligations, with necessary consideration of the sensitivity of children's personal data.

3. Promote this Resolution and its recommendations with stakeholders and policymakers in their jurisdictions and networks.

4. Liaise with relevant international organisations, child-rights-oriented non-governmental organisations and other civil society groups to promote and follow up on the Resolution, including by supporting meaningful participation of children and representing or facilitating their interests where appropriate.

5. Recognise the value the GPA can bring in an international context to contribute to new instruments for governance guidance on AI in education, and reinforce the importance of GPA participation in ongoing initiatives, by sharing data protection and privacy expertise to inform and support global policy development aimed at regulating AI systems within educational environments.

6. Cooperate with each other, the Digital Education Working Group and the AI Working Group to share resources, knowledge and best practices, including creating a list of resources and best practices.

Annexes

This Annex contains three documents offered to provide further alignment with international sources and GPA references, context, explanation and examples related to the Resolution's recommendations:

Document 1 : International sources 1.A and GPA sources 1.B

A Policy Toolbox: Introduction to guidance documents 2 and 3

Document 2: Guidance on AI literacy for students and capacity building for teachers

Document 3: A model Charter for AI use in Educational Institutions

Document 1:

1.A International sources

- United Nations (UN) Committee on the Rights of the Child (CRC) Joint statement on Artificial Intelligence and the Rights of the Child (2026)
- UN Global Digital Compact (2024)
- UN Final Report on Governing AI for Humanity (2024)
- UN CRC General Comment No. 25 on children's rights in the digital environment (2021)
- UNESCO Ministerial Statement Sustaining education as a common good in the age of AI (2026)
- UNESCO Recommendation on the Ethics of Artificial Intelligence (2021)
- UNESCO Beijing Consensus on Artificial Intelligence and education (2019)
- UNICEF's Data Governance for EdTech: Policy Recommendations (2025)
- Organisation for Economic Co-operation and Development (OECD) Recommendation of the Council on Children in the Digital Environment (2021)
- OECD Guidelines for Digital Service Providers (2021)
- OECD Recommendation of the Council on artificial intelligence (2019)
- Council of Europe Recommendation of the Committee of Ministers to member States on artificial intelligence literacy (2026)
- Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (2024)
- Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108+") (2018)
- G20 Digital Ministers' High Level Principles for Children Protection and Empowerment in the Digital Environment (2021)

- G7 Data Protection and Privacy Authorities Roundtable Statement on Promoting Responsible Innovation and Protecting Children by Prioritizing Privacy (2025)
- G7 Data Protection and Privacy Authorities Roundtable Statement on AI and Children (2024)
- G7 Data Protection and Privacy Authorities Roundtable Statement on the Role of Data Protection Authorities in Fostering Trustworthy AI (2024)
- G7 Data Protection and Privacy Authorities Roundtable Statement on Generative AI (2023)

1.B GPA sources

- GPA Resolution on the Collection, Use and Disclosure of Personal Data to Pre-train, Train and Fine-tune AI Models (2025)
- GPA Joint Statement on Building Trustworthy Data Governance Frameworks to Encourage Development of Innovative and Privacy-protecting AI, adopted on the margins of the GPA (2025)
- GPA Resolution on Generative Artificial Intelligence Systems (2023)
- GPA Resolution on Children's Digital Rights (2021)
- GPA Resolution on e-Learning Platforms (2018)
- GPA Declaration on Ethics and Data Protection in Artificial Intelligence (2018)

Introduction to guidance documents 2 and 3

This Resolution addresses the emergence of new AI tools in educational institutions, while remaining consistent with both the 2018 GPA Resolution on e-learning platforms and the 2021 GPA Resolution on Children's Digital Rights. The intention is to reflect the current data governance landscape and recent technological developments in educational settings.

This Resolution provides an opportunity for the global community to revisit the question of edtech with a focus on AI. It is grounded in the findings from the GPA Digital Education Working Group (DEWG) survey (2025/26), during which GPA members shared information such as policy models and guidance documents with the DEWG. Data from the survey provides an overview of the appropriate legal bases and recommendations for processing personal data through AI technologies in the educational context globally.

In the absence of the development and implementation of a comprehensive legal instrument aimed at regulating AI systems in educational settings, collaborating with United Nations bodies such as the Committee on the Rights of the Child, UNESCO and regional organisations such as the Council of Europe, would help harmonise future standards globally.

Moreover, it is essential to bear in mind that AI literacy is not a substitute for digital literacy; rather, it is an extension of it and must be integrated.

To address such shared challenges, education systems will need to orient towards supporting young people to grow up with purpose, agency, awareness, critical thinking, wellbeing, knowledge and skills so that they can shape a better future.

Data Protection Authorities play an important role in educating the public on their data protection and privacy rights.

Given the important role that schools play in the lives of children and families, recent technological developments in AI in edtech should continue to be prioritised in public education efforts.

Based on this GPA Resolution on AI in Education, the GPA community should continue to integrate edtech data governance into its strategic plan and workstreams, including those related to AI and digital education.

Doing this will send a strong signal to governments and industry alike to help foster a coherent global framework and engage in a robust learning agenda.

Policy Toolbox:

Both documents in the Policy Toolbox should be considered as *suggestions* from the GPA/ Digital Education working group (DEWG) and are open to further contextualisation, customisation, and adaptation to meet specific needs and circumstances.

Document 2: Guidance on AI literacy for students and capacity building for teachers

The AI Literacy domain of the Policy Toolbox aims to equip children from different age groups and educational levels with basic data protection, privacy, and education and media literacy foundations. These fundamental skills need to be critically acquired to enable students to become capable, competent, responsible and autonomous individuals who can understand, critique, and shape AI systems and protect students from instrumentalisation.

These skills can be customised where appropriate, for primary and secondary education levels (the first two foundational stages of formal education) before higher education.

Document 3: A Model Charter for AI use in Educational Institutions

The model Charter for AI use in Educational Institutions is written as a pledge for schools and is directed to them. It aims to codify some non-exhaustive fundamental commitments related to the best use of Edtech and AI materials and to demonstrate a strong public commitment to protecting students' digital privacy and strengthening trust in schools. This model Charter provides a privacy-friendly approach to identify principled responsibilities and obligations for schools acting as a controller. It is not intended to replace compliance with obligations under applicable law and can serve as a base model to be modified to reflect local law.

Document 2: Guidance on AI literacy for students and capacity building for teachers

Before considering AI literacy requirements for students, educational institutions should ensure that any AI services used in the educational environment are appropriate for their intended purpose, safe to use, and compliant with the applicable legal framework. AI literacy should not be seen as a substitute for these safeguards.

Basic foundation of digital environmental education for students to be equipped with digital skills on AI from primary to post-secondary schools.

The introduction of artificial intelligence into the educational environment requires students to develop a set of core competencies before they begin working with AI-powered tools. These competencies represent the minimum AI specific literacy that educational authorities and schools, in collaboration with data protection authorities and other stakeholders, should ensure for every student.

- **Understanding the private and public sectors and their differences**

Students need to broadly understand the different interests involved in public- and private- sector actors and how their approach to processing personal data might differ. It is important that when students use AI-related services in an educational environment, those services should be both beneficial to them and compliant with the applicable legal framework governing the processing of personal data. Crucially, when using educational AI technologies and tools such as chatbots, students must recognise when they are interacting directly with a private company that is collecting their information.

Primary school students are able to understand public system: For example, city hall, the public library, firefighters, teachers, roads, buses are public actors. Private sector: businesses or stores aim to make money by selling products or services.

Secondary school students are able to understand that the public sector includes organisations controlled by the state, local governments (regions, departments, municipalities), or public institutions. Their primary mission is to meet collective needs and ensure access to essential services for all, on a non-profit basis. The private sector consists of companies or organisations owned by individuals, shareholders, or investors. Their primary goal is to generate profits while meeting consumer demand.

- **Knowing how to define personal data and sensitive personal data**

Students should be able to define what personal data is (any information that, on its own or in combination with other information, can identify an individual). They should also understand the enhanced protection afforded to special categories of data, including data relating to health, ethnic origin, religious beliefs, sexual orientation, genetic data, and biometric information.

In the context of education, this means recognising that data that may seem harmless at first sight—such as homework assignments submitted, recorded by monitoring software—can fall into these categories. Student data is stored for analysis purposes, which raises important questions about long-term retention and how that data may be used over time.

Furthermore, all participants within the system—including teachers, students, and administrators—are able to add to this data, increasing the risk of inconsistencies or misuse. Most critically, access to this data is not limited to school staff alone, as external organisations may also have access, making it essential to have clear, transparent policies that protect students' privacy and ensure their data is handled responsibly.

Primary school students are able to understand that personal data are all the information that describes them or makes it possible to identify them, not only their name but where they live, what they like to do.

Secondary school students are able to understand that personal data refers to any information that can be used to identify a person, either directly or indirectly.

- **Understanding digital identity**

Students should learn how to create and maintain a healthy digital presence:

  - What is a digital footprint.
  - How their digital footprint is created.
  - Why their footprint matters.
  - How they and others affect their reputation.
  - The right to control their data and manage their online presence.
  - Understand which parts of a digital footprint can be controlled by individuals and which depend on inferences made by companies.
  - Being able to be look ahead to envision their digital identity and build it.

- **Knowing how and why to protect personal data**

Students should learn practical safety and privacy rules, including:

- Use strong and unique usernames and passwords that do not reveal or give access to their identity. If they decide to write their profile description, no information should give clues about who they are, where they live, or what their hobbies are.
- Avoid sharing unnecessary personal data, including profiling information when signing up for artificial intelligence tools.
- Realise that data shared today may be stored, reused, or transferred to third parties for years to come.

Students should be made aware that poorly secured school databases have been the target of cyberattacks, putting the records of thousands of children at risk. Data protection is therefore both a collective and an individual responsibility. If their data is not protected, the consequences can extend far beyond the classroom - affecting students' futures, reputations, and personal safety.

This is why digital literacy must go hand in hand with a genuine culture of data responsibility - one that involves not only students, but teachers, school administrators, and the developers of the tools used in education. Protecting data is not merely a technical matter; it is a fundamental right and a shared obligation in the digital age.

- **Knowing their rights and how to exercise them**

Depending on local data protection and privacy laws, individuals, including minors acting through their legal representatives where applicable, may have rights such as":

- Right of access: knowing what data a platform holds about them.
- Right to rectification: correcting inaccurate data.
- Right to erasure ("right to be forgotten"): requesting deletion when data is no longer necessary.
- Right to restriction of processing: limiting how their data is used in certain circumstances.
- Right to data portability: receiving their personal data in a structured, commonly used, and machine-readable format, and transferring it to another service or platform without hindrance.
- Right to object and automated individual decision-making: refusing certain processing, including profiling.

Schools should make the contact details of the relevant local Data Protection Authority easily accessible to students and their families, and should incorporate complaint simulation exercises into the curriculum.

- **Knowing that the Terms of Use (ToU) should be understandable by anyone**

Providers of AI services should ensure that ToU and privacy policies are clear, accessible and easy to understand, particularly where services are intended for or used by students. This responsibility should not be shifted onto students by expecting them to decipher unnecessarily complex information. As part of their AI literacy, students should nevertheless be equipped with basic skills to identify and understand the key information contained in ToU and privacy policies, including through a structured reading method:

- Identify who the controller is and where it is established.
- Locate the legal basis for each processing purpose.
- Find the data retention period.
- Check whether data is shared with or sold to third parties.
- Identify the mechanism for withdrawing consent (in jurisdictions where it is allowed).

Classroom exercises based on real ToU documents from popular educational AI tools are highly recommended. Where ToU are unavailable in a language accessible to students, this itself constitutes a red flag that should be brought to the attention of school administrators and, if necessary, the data protection authority.

- **Cross-referencing sources**

A vital learning habit for the AI era is systematic source verification. Students should learn to:

- Treat any AI-generated output as a starting point for inquiry, not a conclusion.
- Verify factual claims against at least two independent, authoritative sources - for example, if an AI tool provides a historical date or statistic, the student should confirm it through an encyclopedia, a textbook, or an official institutional website before citing it in their work.

- Understand that AI systems may reproduce the biases present in their training data, and that dominant cultural or linguistic perspectives may be overrepresented.

- **Knowing that AI systems are not infallible**

Students should know about limitations and issues affecting large language models (LLMs), namely sycophancy, hallucinations, the way they work, manipulation and orientations embedded in the LLMs. Especially in the case of children, AI should not be anthropomorphic ('I am feeling, etc').

- **Knowing how to prompt learning systems**

Prompt literacy is the ability to formulate clear, purposeful, and data-minimal queries to AI systems. It is an emerging foundational skill. Students should understand:

- That prompts submitted to external AI services are processed on remote servers and may be used for model training unless the user has explicitly chosen not to allow such use.
- That they should never include personal data (their own or that of others) in prompts unless the service provides explicit, verifiable guarantees of confidential processing - meaning that the platform must not only claim to protect user data, but must demonstrate this through concrete, auditable measures such as published privacy policies compliant with domestic data protection legislation, independent security certifications, or contractual data processing agreements that can be reviewed and used to hold providers accountable.
- That the quality and framing of a prompt directly affect the quality and potential bias of the output.

Document 3: A model Charter for AI use in Educational Institutions

We, , acknowledge that:

1. All children have a fundamental right to privacy and to the protection of their personal data/information.

2. The personal information of children and youth is particularly sensitive and must be protected accordingly in the legal framework governing the processing of personal data.

3. Artificial intelligence tools present tremendous opportunities for student learning and growth, but may also pose significant risks to their privacy.

4. As educators and public institutions, we play a key role in preparing students to use AI tools safely, identify and manage online privacy risks, and become responsible digital citizens.

We pledge to support students through:

Protection

1. Acting in students' best interests, including privacy and safety.

2. Ensuring AI tools in classrooms limit collection, use, and disclosure of students' personal information to only what's necessary for discharging our responsibilities as educators.

3. Ensuring that third-party providers of AI tools and services have strong privacy/data protections, in accordance with applicable laws when procuring, using or otherwise engaging with such tools.

4. Understanding privacy/data protection risks and ensuring that they are mitigated before adopting AI tools and services.

5. Strengthening privacy protections in AI tools and services, including by making privacy-protective settings the default.

6. Informing students, parents, and guardians of significant privacy breaches in a timely way and responding promptly to help mitigate any negative impacts and, where required by local law, also notifying the applicable data protection authority regarding the breach.

Empowerment

1. Providing plain language notices to students, parents, and guardians that comply with the best practices and the data protection or privacy laws of the jurisdiction

2. Explaining what types of personal information is collected and the purposes for which it is used or shared with others in a way that is easy for students, parents, and guardians to understand

3. Providing guidance to students on how to protect their personal information, including any personal information collected by AI tools and services

4. Seeking meaningful feedback from students, parents, and guardians on the use of AI tools and services

5. Informing students of their right to privacy, including their right to access and correct education records containing their personal information with human interaction, and empowering them to exercise these rights

6. Supporting continual awareness of evolving risks and ongoing learning about privacy in the digital environment, including when working with AI tools.

The United States Federal Trade Commission abstains from the adoption of this resolution.