STIAEM

Slow Tech Innovation

AI, Ethics and New Teaching Methods

# Applying the GDPR and Precautionary Principles to Protect Student Identity

Co-funded by the European Union

2025-1-IT02-KA220-SCH-000365213

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them... Project reference code: 2025-1-IT02-KA220-SCH-000365213

Università di Foggia
Studi Umanistici, Lettere, Beni Culturali, Scienze della Formazione

STIAEM

Slow Tech Innovation
AI, Ethics and
New Teaching Methods

Co-funded by
the European Union

2025-1-IT02-KA220-SCH-000365213

eduOpen

**CC BY-NC-SA 4.0 International**

*This license requires that reusers give credit to the creator. It allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, for noncommercial purposes only. If others modify or adapt the material, they must license the modified material under identical terms.*

Università di Foggia
Studi Umanistici, Lettere, Beni Culturali,
Scienze della Formazione

OER 5.1.1: Applying the GDPR and Precautionary Principles to Protect Student Identity
Reference Module: Module 5 - Safety, Privacy and Sustainability
Related Video-Pill: Video 5.1: Precautionary Principle & GDPR Compliance
Authoring partner: Liceo "don Milani" di Acquaviva delle Fonti - sede associata "Da Vinci" di Cassano delle Murge
Topic / Thematic Focus: GDPR application, precautionary principles and student identity protection

## Introduction and Learning Objectives

This resource, together with OER 5.1.2, accompanies video-pill 5.1 “Precautionary Principle & GDPR Compliance” of Module 5 - Safety, Privacy and Sustainability. Its purpose is to offer teachers an operational guide for applying the precautionary principle and the General Data Protection Regulation (GDPR) to schools, protecting the digital identity of students.
The text connects to DigComp 3.0 (Cosgrove & Cachia, 2025), whose Area 4, “safety, wellbeing and responsible use”, includes competence 4.2 “Protecting personal data and privacy”; to the “AI ethics” pillar of the UNESCO framework for teachers (Miao & Cukurova, 2024); and to the principles of Slow Tech (Patrignani & Whitehouse, 2019) that inspire the STIAEM model. The main legal references are Regulation (EU) 2016/679 (GDPR) and Regulation (EU) 2024/1689 (AI Act).
By the end of the reading, teachers will be able to:

- recognise when the use of an AI system in an educational context falls into the high-risk category and requires reinforced safeguards;
- identify the correct legal basis for processing and apply the principles of lawfulness, minimisation and purpose limitation;
- put in place the essential safeguards — impact assessment, human oversight, information — to protect students' identity.

## 1. The precautionary principle applied to schools

The precautionary principle is not a prohibition, but a rule of prudence proportionate to risk: when an activity may produce serious and not entirely foreseeable harm, action is taken before the harm occurs, adopting measures commensurate with what is at stake. The AI Act translates this logic into a risk-based approach and explicitly classifies the use of AI in education among high-risk systems.
“AI systems used in education or vocational training, in particular for determining access or admission, for assigning persons to educational and vocational training institutions or programmes at all levels, for evaluating learning outcomes of persons, for assessing the appropriate level of education for an individual and materially influencing the level of education and training that individuals will receive or will be able to access or for monitoring and detecting prohibited behaviour of students during tests should be classified as high-risk AI systems, since they may determine the educational and professional course of a person's life and therefore may affect that person's ability to secure a livelihood” (AI Act, Reg. (EU) 2024/1689, recital 56).

The consequence for schools is precise: whoever adopts one of these systems becomes a “deployer”, that is, a responsible user, and must use it according to the instructions, assign effective human oversight and monitor its operation.
“Deployers of high-risk AI systems shall take appropriate technical and organisational measures to ensure they use such systems in accordance with the instructions for use accompanying the systems” and “Deployers shall assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support” (AI Act, Art. 26, paras. 1-2).
In practice, precaution at school means three choices: preferring less intrusive tools when they perform the same didactic function; avoiding functions of profiling or automatic assessment of the student; documenting decisions, so that they are verifiable and open to discussion. This is not a bureaucratic burden, but the way in which the school takes responsibility for what it introduces into the classroom.

## 2. The GDPR and student data

The GDPR applies to any processing of students' personal data: name, grades, photographs, voice recordings, images of the face, up to biometric data. It does not concern only the school office records, but also the digital tools that teachers use in the classroom. Two principles of Article 5 establish its underlying logic.
“les collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (...) ('purpose limitation'); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')” (GDPR, Reg. (EU) 2016/679, Art. 5, para. 1, letters b and c).
The third paragraph, on the other hand, concerns responsibility: those who decide how and why data are processed must be able to demonstrate it. This is the principle of accountability, which in schools rests on the institution and, for the teaching part, on the teacher.
“The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')” (GDPR, Art. 5, para. 2).
Special attention is due to minors, because their condition of greater vulnerability is explicitly recognised by the European legislator.
“Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data” (GDPR, recital 38).
From this follows an immediate didactic consequence: before introducing an application that collects student data, the teacher asks not only whether it “works”, but what data it collects, for what declared purpose and for how long it keeps them.
The UN Committee on the Rights of the Child calls on States to protect children and their data in the digital environment (UN OHCHR, 2021). In the same direction, the Council of Europe invites States to respect, protect and fulfil the rights of minors in the digital space (Council of Europe, 2018).

## 3. Few-Shot Prompting and the Pedagogical Logic of Worked Examples

Processing is lawful only if it rests on one of the conditions laid down in Article 6. It is not enough for the data to be useful: an explicit legal reason is required.

“Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (...) (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child” (GDPR, Art. 6, para. 1).

When the basis is consent and the service is offered directly to a minor, the minimum age comes into play. In Italy the reference threshold for information society services is set at 14 years, with the possibility — provided for by the regulation — of going down to no lower than 13.

“the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years” (GDPR, Art. 8, para. 1).

For the teacher this translates into a practical rule: enrolling an entire class on a commercial platform “because it is convenient” is not a legal basis. It is necessary to check the service's minimum age, the terms of use and, where required, parental consent; or else to choose institutional solutions that do not require personal data.

### 4. Impact assessment and human oversight

When a processing operation may present a high risk to the rights of data subjects, the GDPR requires an impact assessment in advance. It is the most concrete safeguard of the precautionary principle.

“Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data” (GDPR, Art. 35, para. 1).

The assessment becomes mandatory, among other things, when personal aspects are evaluated systematically with automated decisions — that is, when the student is profiled in order to guide or assess them.

“a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person” (GDPR, Art. 35, para. 3, letter a).

The framework is completed by the obligation of human oversight laid down by the AI Act for high-risk systems: the machine must be able to be supervised by people during its use.

“High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use” (AI Act, Art. 14, para. 1).

The two regulations go together: the AI Act establishes that, where applicable, the user relies on the information provided by the provider to comply with the impact assessment required by Article 35 of the GDPR (AI Act, Article 26, paragraph 9). Assessment and oversight are not separate obligations, but a single safeguard of guarantee.

## 5. In the classroom: an operational protocol for student identity

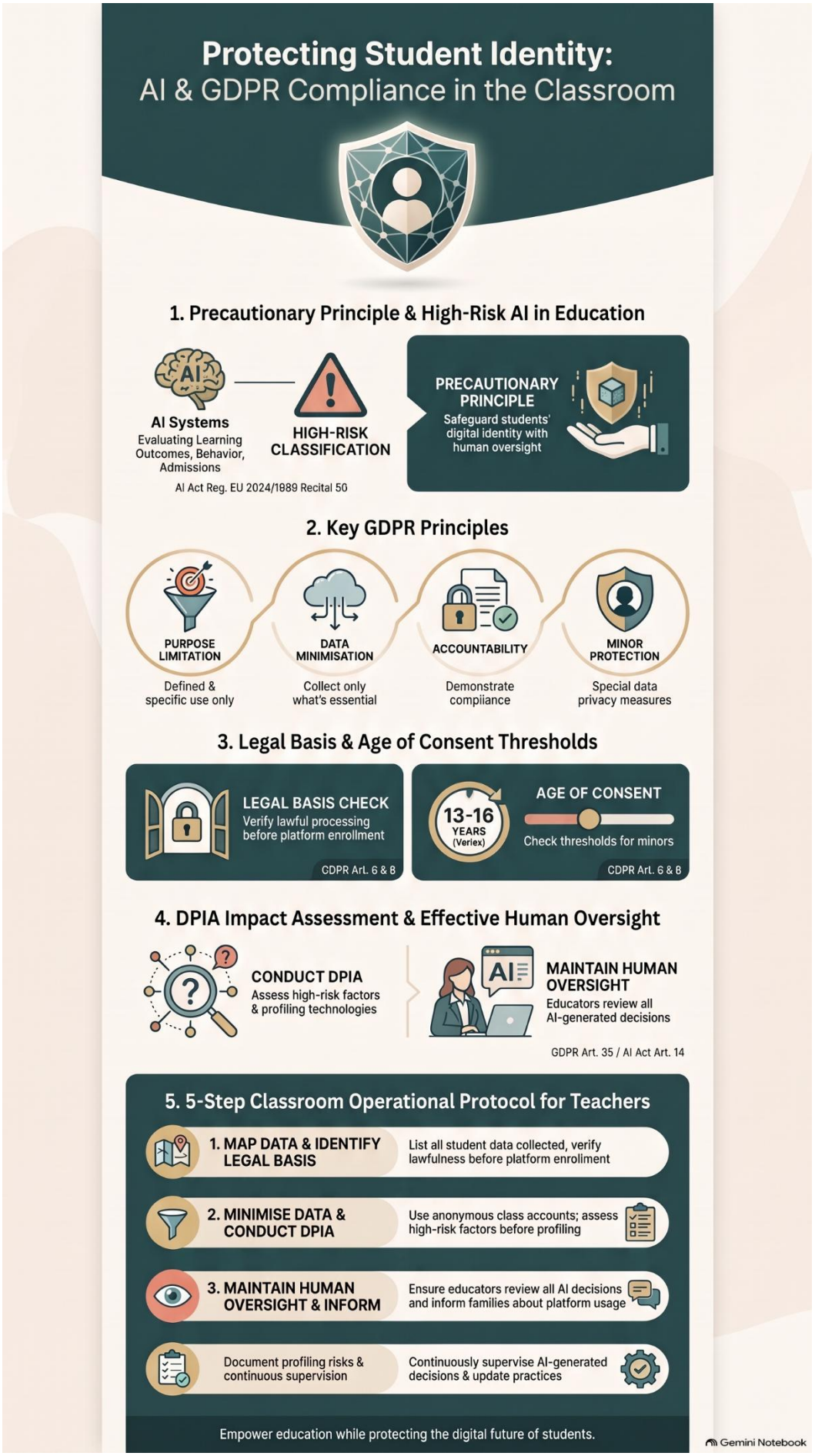
From the foregoing a five-step protocol can be derived, usable before introducing an AI tool. First: map the data, that is, list which personal information enters the system. Second: identify the legal basis for the processing. Third: minimise, removing what is not needed. Fourth: if the risk is high, prepare the impact assessment and share it with the school. Fifth: guarantee human oversight and information to students and families.

An example. A teacher wants to use an adaptive platform that assigns exercises based on students' answers. Applying the protocol: the data map shows that the system records times, errors and individual progress; the legal basis is the performance of a task in the public interest or consent, to be verified with the institution; minimisation suggests working on class accounts, without personal details; the impact assessment is required because the system profiles students; human oversight requires that the assignment of paths remain a proposal that can be revised by the teacher.

The following table summarises the safeguards and their practical application.

| Safeguard | Reference | What it requires of the teacher | Classroom example |
|---|---|---|---|
| Legal basis | GDPR Art. 6 | Identify a condition of lawfulness before processing the data | Check the terms of use before enrolling the class in a service |
| Minimisation and purpose | GDPR Art. 5.1.b-c | Collect only the data necessary, for the declared purpose | Use class accounts without students' personal details |
| Consent of minors | GDPR Art. 8 | Check the minimum age and parental consent | Check the age required by the service before enrolment |
| Impact assessment | GDPR Art. 35 | Assess risks and safeguards before high-risk processing | Document the risks and mitigations of a platform that profiles |
| Human oversight | AI Act Arts. 14, 26 | Maintain effective human control and use the systems as intended | Always review automatic decisions that weigh on students |

## Visual Scaffolding



## Conclusions and Metacognitive Reflection Prompts

This resource has shown how the precautionary principle and the GDPR converge in a single professional duty: to protect students' identity when using AI tools. The AI Act classifies as high-risk the AI in education that affects the life paths of students; the GDPR sets out the principles of lawfulness, minimisation and purpose limitation, with reinforced protection for minors and the obligation of impact assessment. The common thread is documented responsibility and human oversight.

To transfer these core ideas into one's own practice, the following reflection prompts are proposed:

- Which personal data of students currently enter the digital tools you use, and could you indicate their legal basis?
- In which situations of your teaching does an automatic system affect a student's path, and how do you guarantee human oversight?
- How would you explain to a class, in simple terms, why “collecting less data” is also a form of respect?

## Technical Metadata Sheet

| Metadata Field | Specification / Parameter Value |
|---|---|
| **Identifier** | OER 5.1.1 |
| **Title** | Applying the GDPR and Precautionary Principles to Protect Student Identity |
| **Creator** | Liceo "don Milani" di Acquaviva delle Fonti - sede associata "Da Vinci" di Cassano delle Murge |
| **Description** | The resource applies the precautionary principle and the GDPR to the educational use of AI, focusing on the protection of student identity. It explains when an AI system used in education falls into the high-risk category, how to identify the correct legal basis, and how to apply lawfulness, minimisation and purpose limitation. The practical focus is on the essential safeguards — impact assessment, human oversight and information — and on an operative classroom protocol. |
| **Keywords** | GDPR; precautionary principle; student data protection; high-risk AI; legal basis; data minimisation; impact assessment; human oversight |
| **Language** | EN (English) |
| **Affiliation** | Liceo "don Milani" di Acquaviva delle Fonti - sede associata "Da Vinci" di Cassano delle Murge |
| **Contributor** | STIAEM Transnational Scientific Board (peer review, Rhodes validation protocol) |
| **Media Format** | Text; Infographics |
| **Genre** | Training Manual; Educational Guide |
| **URL** | |
| **Citation** | Cosgrove, J., & Cachia, R. (2025). DigComp 3.0: European digital competence framework (Fifth edition). Publications Office of the European Union. https://data.europa.eu/doi/10.2760/0001149<br>European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1-88. https://eur-lex.europa.eu/eli/reg/2016/679/oj<br>European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L, 12.7.2024. https://eur-lex.europa.eu/eli/reg/2024/1689/oj<br>Miao, F., & Cukurova, M. (2024). AI competency framework for teachers. UNESCO. https://doi.org/10.54675/ZJTE2084<br>Patrignani, N., & Whitehouse, D. (2019). Slow tech: The bridge between computer ethics and business ethics. In This changes everything - ICT and climate change (pp. 265-280). Springer.<br>United Nations - OHCHR. (2021). General Comment No. 25 (2021) on children's rights in relation to the digital environment. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation<br>Council of Europe. (2018). CM/Rec(2018)7 - Guidelines to respect, protect and fulfil the rights of the child in the digital environment. https://search.coe.int/cm?i=09000016808d96d3 |
| **Educational Level** | Secondary School |
| **Associated Module / MOOC Video Lesson** | Module 5 - Safety, Privacy and Sustainability / Video 5.1 - Precautionary Principle & GDPR Compliance |
| **Learning Objectives** | recognise when the use of an AI system in education falls into the high-risk category and requires reinforced safeguards; identify the correct legal basis for processing and apply the principles of lawfulness, minimisation and purpose limitation; put in place the essential safeguards - impact assessment, human oversight, information - to protect students' identity. |
| **Rights** | Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) |
| **Date Available** | 14/09/2026 |

| Date Modified | |
|---|---|

## References and Webography


Cosgrove, J., & Cachia, R. (2025). DigComp 3.0: European digital competence framework (Fifth edition). Publications Office of the European Union. https://data.europa.eu/doi/10.2760/0001149

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1-88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L, 12.7.2024. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Miao, F., & Cukurova, M. (2024). AI competency framework for teachers. UNESCO. https://doi.org/10.54675/ZJTE2084

Patrignani, N., & Whitehouse, D. (2019). Slow tech: The bridge between computer ethics and business ethics. In This changes everything - ICT and climate change (pp. 265-280). Springer.

United Nations - OHCHR. (2021). General Comment No. 25 (2021) on children's rights in relation to the digital environment. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

Council of Europe. (2018). CM/Rec(2018)7 - Guidelines to respect, protect and fulfil the rights of the child in the digital environment. https://search.coe.int/cm?i=09000016808d96d3