1.6 Legislation

Take Home message

- **The EU AI Act is the legal basis.** The EU's rulebook for AI is in force since August 2024 and phasing in through 2027. It applies not just tech companies, but also to schools.
- **AI literacy is a duty, not a course to tick off.** Schools must support staff in building AI literacy.
- **Several AI uses are banned outright.** Among them: inferring students' emotions from facial or vocal data, AI that exploits children's vulnerabilities to distort their behaviour, and building facial-recognition databases or inferring traits like race or religion from biometric data.
- **Risk depends on the decision, not the product.** Ordinary writing, research, translation and lesson-planning tools are not high-risk simply because they are used at school. They become high-risk once they influence admission, learning pathways, exam outcomes or employment decisions.
- **Not everything AI-generated needs a label.** The disclosure duty mainly sits with the provider; teacher-reviewed material with human editorial control is exempt.
- **High-risk AI needs a human who can overrule it.** AI output is never the final decision. You must understand its limits and be able to disregard or override it.
- **The AI Act sits on top of other law, it doesn't replace it.** National data protection, education, employment, child protection and copyright law continue to apply alongside it.
- **The GDPR governs the data, not just the tool.** Even an AI system that is fine under the AI Act can still be off-limits if it processes personal data about students or staff without a valid legal basis.

> If you remember only one sentence from this page: **Use AI to support your professional judgement, not replace it—stricter rules apply as soon as AI helps make decisions about grades, educational pathways or people.**

The EU AI Act

The EU AI Act (Regulation (EU) 2024/1689) is the EU's single, risk-based rulebook for artificial intelligence. Instead of regulating specific products, it classifies AI systems by the risk they pose and attaches obligations accordingly — from an outright ban for a small set of practices, through extra duties for "high-risk" uses, to no special rules at all for everyday tools. It applies directly in

every member state, to public and private organisations alike.

The Act phases in step by step. It has applied since 1 August 2024; since 2 February 2025, the banned practices below and the duty to build AI literacy (Art. 4) are already binding; from 2 August 2026, most of its remaining provisions apply.

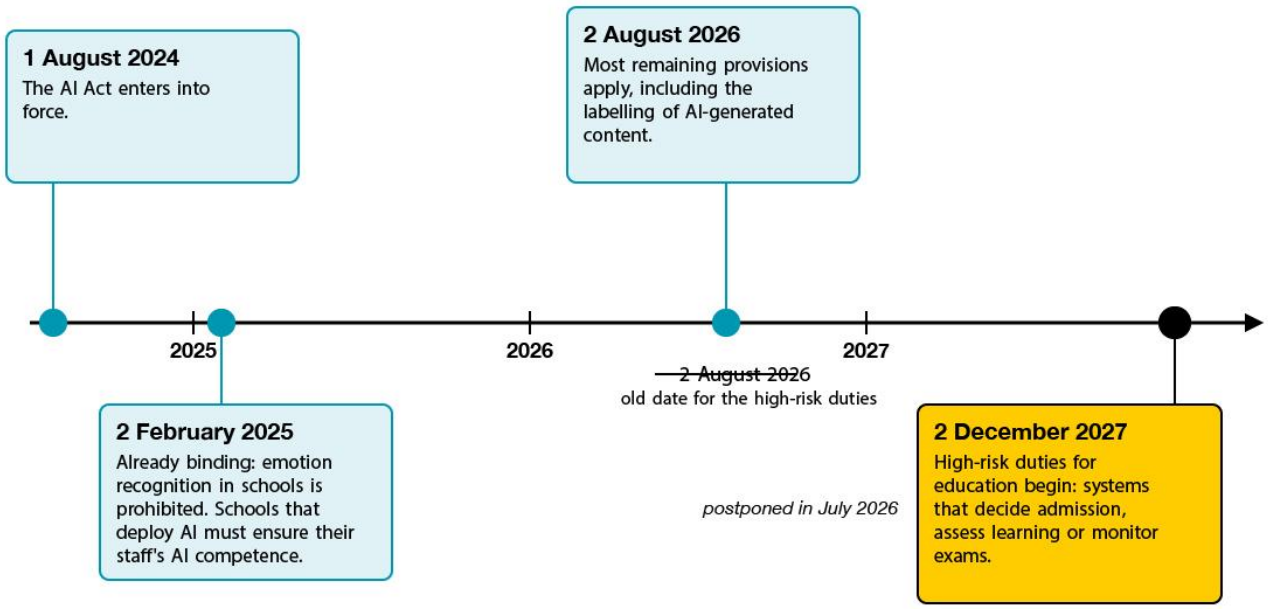


Fig. 1: The "AI roadmap" (Image generated with ...)

Who is responsible for the use of AI?

If a school introduces and controls an AI system, the school or school authority is usually the *deployer* (Art. 3(4)). The teacher is normally not a separate deployer when using the tool under the school's instructions, but must still follow those instructions and all relevant school and data-protection rules.

Teachers need to know what they are using

Schools and school authorities must take appropriate measures to support the development of AI literacy among those who use AI systems on their behalf (Art. 4). The AI Act does not specify a particular level of competence, certificate or training format. These rather depend on the AI system

used, how it is used, and who may be affected.

AI practices banned outright for schools

The AI Act bans eight AI practices outright (Art. 5); four of them are directly relevant to schools:

1. Using AI systems in educational institutions to **infer emotions or intentions from biometric data** (such as students' facial or vocal characteristics) is generally forbidden. Narrow exceptions exist for medical or safety purposes (Art. 3(39); Art. 5(1)(f)).
2. AI systems that exploit someone’s vulnerabilities due to age (as with children), disability, or social or economic situation, in a way that distorts their behaviour and causes them harm, are banned regardless of intent (Art. 5(1)(b)).
3. Building or expanding a facial-recognition database through untargeted scraping of images from the internet or from CCTV footage is banned. This is relevant if a school considers a facial-recognition tool for attendance or exam monitoring (Art. 5(1)(e)).
4. Using biometric data to categorise people in order to infer protected traits such as race, political opinions, religion or sexual orientation is banned. This is relevant for any biometric-based tool, such as exam-proctoring software, that goes beyond its stated purpose (Art. 5(1)(g)).

Does AI-generated content always need a label?

If students interact directly with an AI system, such as a chatbot, they must be informed that they are interacting with AI. Usually the system provider is responsible for making this clear (Art. 50(1)).

Schools and teachers must disclose deepfakes, or AI-generated text published on matters of public interest, when these are used in the classroom (Art. 50(4)). This requirement does not apply where the AI-generated content has undergone effective human review or editorial control, and a person or institution assumes editorial responsibility for its publication. An AI-assisted worksheet reviewed by a teacher therefore does not automatically require a label.

When AI in education becomes high-risk

Ordinary writing, translation, research and lesson-planning tools are not high-risk simply because they are used for work. Classification depends on the system's intended purpose, not simply on which product is used (Art. 6 · Annex III).

AI systems may be classified as high-risk when they are intended to:

For Teachers	For Schools
• decide about students' access, admission or assignment to educational or vocational institutions and programmes; • evaluate students' learning outcomes or steer their learning processes; • assess the appropriate level of education a student will receive or can access; or • detect students' prohibited behaviour during examinations. *(Annex III, point 3)*	• recruit or select teachers, including screening applications; • decide on contract terms, promotion or termination of a teacher's employment; • allocate tasks based on a teacher's behaviour or personal traits; or • evaluate teachers' performance. *(Annex III, point 4)*

A limited checking or preparatory tool may also fall outside the high-risk category if it does not significantly influence a decision. However, an education system that profiles individuals is always considered high-risk.

What high-risk AI means for schools and teachers

Classification of an AI system as high-risk does not automatically rule it out from use in schools. But high-risk systems come with obligations (Art. 26):

These obligations for high-risk AI in education apply from **2 December 2027** — but the prohibitions above and the AI-literacy duty already apply today.

For Teachers	For Schools
• use it only for its approved purpose and follow its instructions; • do not treat its output as a final decision; • understand its main limitations and likely sources of error; • watch for overreliance on apparently convincing results; and • be prepared to disregard or override its output.	• provide competent and authorised human oversight; • ensure that any input data under its control is relevant and sufficiently representative; • monitor the system and respond to risks or serious incidents; • keep automatically generated logs for at least six months where those logs are under its control; and • inform students, teachers or affected people in advance when the system assists decision-making about them.

Public bodies and private organisations providing public services may also have to complete a fundamental rights impact assessment before using high-risk AI (Art. 27). Public authorities and organisations acting on their behalf may additionally have to register the system in the EU database (Art. 49). Whether this is the responsibility of the school or its governing authority depends on the national school system.

The AI Act is not the only law that matters

The AI Act does not replace european or national regulations on data protection, education, employment and worker participation, child protection or copyright (Art. 2(7)). For example, the fact that a tool is not high-risk does not mean that you may upload students' work or personal data to it.

A tool may be acceptable under the AI Act but still prohibited by data-protection law or your school's rules.

The GDPR

The GDPR (Regulation (EU) 2016/679) is the EU's law on data protection. It plays a supporting role alongside the AI Act: while the AI Act asks whether and how an AI system may be used at all, the GDPR asks a narrower question — may this particular data about this particular person be processed this way? Meeting one does not automatically mean you have met the other.

- **It applies as soon as personal data is involved.** Names, school email addresses, student work, voice recordings, transcripts, photos, grades, attendance and learning-progress data all count as personal data (Art. 4). Most AI tools used in class touch at least one of these.
- **You need a lawful basis to process it.** A legal obligation or a task carried out in the public interest are the bases schools usually rely on; consent is also possible but must be freely given and, for younger students, given by a parent or guardian (Art. 6, Art. 8).
- **Some data needs extra protection.** Health information, biometric data and data revealing racial or ethnic origin, religion or similar traits are "special category data" and are, in principle, off-limits without a specific exception (Art. 9) — one reason the AI Act separately bans several biometric-inference practices in schools.
- **Know who is responsible.** The school is normally the "controller"; an AI provider processing data on the school's behalf is a "processor" and needs a data-processing agreement that spells out its obligations (Art. 28). Check this before rolling a new tool out school-wide.
- **Data leaving the EU needs a safeguard.** Many popular AI tools are hosted outside the EU. Personal data may only travel there if an adequacy decision or another approved safeguard, such as standard contractual clauses, is in place (Art. 44).

- **Students and staff keep their rights.** They can ask what is held about them, have it corrected or deleted, and object to decisions based solely on automated processing that significantly affects them (Art. 15–Art. 22) — a right that runs alongside, and reinforces, the AI Act's human-oversight requirements for high-risk systems.

In practice: before feeding real student or staff data into an AI tool, check that your school has approved it, share no more personal data than the task needs, and prefer anonymised or fictional examples when just trying a tool out.

Where to find help

Enforcement is organised differently in each EU country. Because national responsibilities may change, use the European Commission's current list of national market-surveillance authorities. Anyone (a teacher, a student, a parent) can lodge a complaint with that authority if they believe the Act has been breached (Art. 85). Where a high-risk system, such as an admission or exam-monitoring tool, has led to a decision that significantly affects a student, they (or their parents) can also ask for an explanation of that individual decision (Art. 86).

National rules for your country

The AI Act is EU-wide, but enforcement bodies, school law and data-protection practice differ by country. Country-specific notes for the Playbook's partner countries will be added here:

- Austria
- Czechia
- Germany
- Latvia
- Poland
- Slovakia
- Slovenia
- Spain

Revision #1
Created 2026-10-20 11:34:13 UTC by Jannik
Updated 2026-10-20 11:34:13 UTC by Jannik