

AI + Student Work: What Every School Must Know

For EU/UK institutions (and relevant globally)

Core message:

Removing names from student work is **not enough**. Uploading it into ChatGPT, Gemini, or any LLM without safeguards is **non-compliant** with GDPR, the EU AI Act, and child protection laws.

GDPR & Parental Consent

- Under **GDPR Article 8**, EU countries set their own digital consent age (13–16).
 - Example: **France = 15 years** (French Data Protection Act, Act No. 78-17).
- Children under that age require **parental consent** before their work enters an AI system.
- Consent must be: **specific, informed, and renewed** if the system or provider changes.

EU AI Act = High Risk

- Entered into force August 2024. **Full compliance by August 2026**.
- Education = **high-risk domain** (Article 6, Annex III; Recital 56).
- Schools must:
 - Protect children as a vulnerable group
 - Ensure age-appropriate transparency
 - Conduct risk assessments and oversight

Not all AI use in education is considered “high-risk”. It is classified as **high-risk when AI is used to influence, grade, assess, or make decisions that affect a child’s access to education, opportunities, or progression**.

This includes:

- **Grading and feedback** on student work
- **Automated admissions or placement** decisions
- **Monitoring or profiling** of student behavior or performance
- **Assessment of eligibility** for educational services

By contrast, **low-risk uses** might include AI-supported spelling suggestions or basic productivity tools, where no significant decision about a child is made.

Mandatory AI Literacy Training

Staff training must cover:

- Ethical use of AI in schools
- Oversight and accountability
- Risks: bias, misinformation, privacy
- Consent and governance rules

Institutional Readiness Checklist

Before uploading student work to an AI system, leaders must be able to answer **YES** to:

1. Do we know the legal age of consent in our country?
2. Have we obtained informed parental consent?
3. Have we conducted an AI-specific DPIA?
4. Do we have binding contracts with providers?
5. Is human oversight clearly defined?
6. Can we explain AI use to children and parents?
7. Has staff completed AI ethics/governance training?
8. Do we keep compliance/audit records?
9. Do we have an exit plan if risks emerge?

Bottom line:

AI literacy is not enough. **AI responsibility is the standard.**

AI in Education: Why Anonymization is Not Enough

Briefing Note for Staff

Introduction

A common misconception is that removing names from student work makes it safe to upload into ChatGPT, Gemini, or other LLMs. This is incorrect. In the EU/UK, education is a high-risk AI use case. Regulations require strict safeguards, not just “anonymization.”

GDPR & Parental Consent

- GDPR Article 8 allows Member States to set the age of digital consent. Ranges: 13–16.
 - E.g. France requires 15 (Act No. 78-17 of 6 January 1978).
- Children below this age cannot legally consent. Parental permission is mandatory.
- Consent must be:
 - Specific to the exact system use
 - Informed so parents understand risks
 - Renewed if schools switch AI systems or if providers add new LLM functions

Example: A French school uploads anonymized essays into Gemini without parental consent. Despite removing names, this is unlawful. Consent must come from parents, not just students, until age 15.

EU AI Act: High-Risk in Education

- The EU AI Act (in force Aug 2024, compliance Aug 2026) explicitly treats many forms of AI use in education as high-risk.
- Relevant provisions:
 - Article 6 + Annex III: grading, feedback, and assessment = high risk
 - Recital 56: explains why education is covered
 - Article 5: protection of children as vulnerable group
 - Article 50: AI communication must be age-appropriate
- Implication: Institutions cannot use external AI for student work without risk assessments, oversight, and governance processes.

Mandatory AI Literacy & Ethics Training

AI Literacy training is mandatory for all staff. Additionally, because much of the AI used in education is high-risk, staff cannot use this type of AI without prior training.

This training should cover:

- AI capabilities and limitations
- Ethical risks: bias, stereotyping, child safety
- Consent management and governance procedures
- Oversight: teachers must remain accountable for decisions
- Transparency: how to explain AI use to parents and children

Note: Training is not optional. It is part of compliance obligations.

Governance Requirements Before AI Use

- Conduct a Data Protection Impact Assessment (DPIA) tailored to AI
- Identify and document a legal basis for processing student work
- Secure provider contracts covering retention, deletion, and third-party access
- Define human oversight roles: teachers remain responsible for evaluation
- Ensure record-keeping for compliance audits
- Prepare an exit strategy if the provider changes terms or risks escalate

International Perspective

- US: State-level laws (e.g., Colorado AI Act, California child data protections) are moving toward EU-style rules
- Canada: Artificial Intelligence and Data Act (AIDA) requires governance of high-impact systems
- Australia: Draft AI safety frameworks already highlight education as high-risk

Implication: Schools outside the EU/UK should not assume a free pass. The same standards are arriving worldwide.

Institutional Readiness Checklist

(see printable version below)

Conclusion

Uploading student work to an LLM without safeguards is non-compliant, unsafe, and unethical.

Schools must treat AI as a high-risk technology; with training, consent, oversight, and governance in place.

The shift is clear: AI literacy is not enough. AI Governance is the standard.

AI Use in Education: Compliance Readiness Checklist

Education = High-Risk Domain under the EU AI Act. Compliance is not optional.

Consent & Legal Basis

- ☐ Confirm the **age of digital consent** in your country (13–16 under GDPR).
 - ☐ Obtain **specific and informed parental consent** where required.
 - ☐ Verify a valid **legal basis** for processing student work.
-

Risk & Oversight

- ☐ Complete an **AI-specific Data Protection Impact Assessment (DPIA)**.
 - ☐ Ensure **human oversight**: teachers, not AI, make the final judgments.
 - ☐ Keep an **audit trail** of risks, safeguards, and decisions.
 - ☐ Prepare an **exit strategy** if the AI system or provider changes.
-

Contracts & Providers

- ☐ Have **binding contracts** with AI providers covering data use, storage, and deletion.
 - ☐ Check whether the provider **introduces new LLM functions**. If so, seek renewed consent.
-

Training & Transparency

- ☐ Provide **mandatory AI literacy & ethics training** for all staff.
- ☐ Ensure staff can explain AI use in **age-appropriate language** to students and parents.

Bottom Line:

Anonymizing names is **not enough**. AI in education requires **consent, training, oversight, and governance**.

Move from AI *literacy* to **AI responsibility**.