INSTAGE January 2026

InStage Responsible AI Principles

InStage is committed to the responsible development and use of artificial intelligence. AI is a core part of the InStage experience, and we design it to be trustworthy, safe, and aligned with institutional expectations. These principles guide how we approach AI in our business.

Privacy

InStage prioritizes the privacy rights of students and institutions. **We do not use customer content to train AI models.** AI uses only the information needed to perform the requested task, and data is handled under defined retention and confidentiality practices consistent with our commitments in our Privacy Policy.

Transparency

InStage designs AI outputs to be interpretable and clearly communicates when AI is involved in an experience. We provide procurement-ready documentation for institutional due diligence and communicate that AI outputs can be incomplete or wrong and should be reviewed before being relied upon.

Human-in-the-Loop

AI supports decisions but does not make high-stakes decisions on its own. InStage is not intended to make final, consequential decisions about individuals without human review. **Educator judgment remains central,** and AI-generated feedback is designed to support learning reflection, not replace instructor evaluation.

Security

InStage treats AI features as part of our security program. AI features follow the same engineering, testing, and change-control expectations as the rest of the platform. We maintain security monitoring and an incident response process, and AI providers are vetted through third-party risk management practices.

Fairness

InStage works to reduce the risk that AI behaves differently for different people in harmful or unjustified ways. We design prompts and evaluation approaches to reduce avoidable bias, assess AI behavior for quality and fairness signals, and avoid designing AI to be the sole determinant of a learner's evaluation.

Governance & Accountability

Responsible AI requires clear ownership and repeatable processes. AI risk and governance have clear internal ownership across leadership, security, and product. New AI capabilities are reviewed for privacy, security, and user impact before rollout, and we review AI performance and emerging risks over time.

What We Do Not Do

- We do not use customer content to train AI models.
- We do not use AI for facial recognition, eye tracking, or biometric identification.
- We do not allow unapproved AI tools to process customer personal data.
- We do not represent AI outputs as guaranteed, final, or authoritative.

Questions or institutional reviews: privacy@instage.io · instage.io/trust