White Paper – AI Safeguarding, Security and Privacy

Last updated April 23, 2026

Introduction

At Kognity, we are committed to providing all students with modern, engaging, and high-quality learning experiences. As part of our vision to radically improve learning for the world's students, we continuously explore how technology - including artificial intelligence ("**AI**") - can enhance teaching and learning outcomes.

The integration of AI into the Kognity Teaching & Learning Platform represents a natural evolution of our pedagogical approach. However, with this advancement comes responsibility. We recognise that trust is fundamental in education, and we are committed to ensuring that AI is implemented in a way that is transparent, secure, and aligned with the needs of students and educators.

We got you - Our commitment to safeguarding AI

We are committed to ensuring that AI is used responsibly and in a way that protects the rights, privacy, and integrity of all users of the platform.

AI functionality in Kognity is designed to:

- Support educators in their professional judgment, not replace it
- Enhance learning outcomes and feedback quality
- Operate within the same strict data protection and security frameworks as the rest of the platform

We will never:

- Use AI to make **fully** automated grading decisions without human oversight
- Use student data for **advertising**, **profiling**, or **non-educational purposes**
- **Sell** or **monetise** AI-derived insights from Platform Data

Our use of AI is governed by our Standard Subscription Agreement Terms, Privacy Policies, and applicable laws, including FERPA, COPPA, GDPR, EU AI Act, and relevant state-level legislation.

AI is built on our privacy-first foundation

Kognity has a strong foundation in rigorous data protection practices. These principles extend directly into how we design and deploy AI.

AI functionality is developed in accordance with:

- Privacy by Design and least privilege access
- Strict internal governance and review processes
- Alignment with established frameworks such as SOC2, ISO27001, ISO42001, and NIST

AI is not a separate layer - it operates within the same trusted foundation as the rest of the Kognity platform.

Your data remains Your data

To deliver AI-supported functionality, Kognity processes limited School Data. As with all school data within the platform, this remains under the control of the school.

AI features operate on:

- Student-submitted content only (e.g. assignment responses)
- Not on personally identifiable information ("**PII**")

We do not include PII in any requests to large language models ("**LLMs**") or external AI services, and **we do not use** student data to train general-purpose AI models.

Transparency and control - supporting you with confidence

We believe that AI should be understandable and controllable. Therefore, we ensure that:

- Where appropriate, AI-generated outputs may be accompanied by supporting context or rationale to help educators evaluate and interpret them
- Educators retain full control over final decisions

To support accountability and transparency, Kognity maintains traceability of AI interactions through internal logging and monitoring systems. These logs provide visibility into:

- The context of AI usage within the platform
- The interaction between the user and the AI feature
- The resulting output and system behaviour

This ensures that AI-supported actions are auditable, traceable, and aligned with platform usage and governance requirements, without exposing sensitive data.

Security of AI systems

AI functionality is protected by the same robust security framework as the Kognity platform.

Our controls include:

- Encryption in transit and at rest for all processed data

- Role-based access controls and least-privilege principles
- Continuous monitoring of systems and infrastructure
- Regular vulnerability scanning and penetration testing
- Secure development practices, including testing and code review

AI operates within our controlled infrastructure and does not introduce additional exposure to user data.

Fairness, safety and responsible use

We are committed to ensuring that AI is used in a fair, safe, and educationally appropriate way. Therefore:

- AI systems are designed to minimise bias and unintended outcomes
- Outputs are continuously evaluated and scrutinized
- Content is constrained to educational use cases

Human oversight remains a core safeguard in all AI-supported features.

Continuous improvement

We continuously:

- Monitor performance and outcomes
- Improve models and safeguards
- Review compliance with emerging regulations and standards

We are committed to transparent communication with our customers regarding any material changes to AI functionality.

Questions?

We're happy to share further insights into our AI safeguarding, security, and privacy practices.

Please contact your Kognity representative or email us at:

dataprotection@kognity.com

We look forward to responsibly improving learning together with You.