How to Meet the **Next Wave of Students' Demands**

Strategic preparation for AI and supporting infrastructure ensures a solid, secure foundation for all that's to come.

From AI tutors or chatbots that aid marketing and recruiting, to all manner of academic research and experimentation, there's little question that AI is playing an outsized role in how colleges and universities deliver the student experience. As students come onto campuses fully AI-aware, they increasingly expect to engage with AI-driven or -enabled applications and tools, from the dorm to the classroom and everywhere in between. Beyond bolstering the broader campus infrastructure and environment to meet those expectations, IT teams must work closely with SecOps, data owners, and other stakeholders to ensure every new AI initiative is built on a solid, secure, and sustainable foundation.

PRODUCED BY: CAMPUS TECHNOLOGY

SPONSORED BY: CLOUDFLARE

Campus Technology recently spoke with Dan Kent, field CTO at Cloudflare, about how to approach those needs as institutions push to prepare students for a not-so-distant future in which they engage with, and build, new AI tools and applications themselves. A protect, connect, accelerate, and build framework puts colleges and universities on the right path to providing exceptional student experiences and delivering on AI's promise, Kent said. Here's the work each of those stages should include, and tools to help get started.

Protect Everything

As AI delivers new efficiencies and ways of approaching students' work in class, it also propels the same efficiencies for hackers and other bad actors, who can now craft more convincing phishing e-mails or write malicious code faster, cheaper, and more effectively than ever before. Such grave risks require greater protections, not only through establishing proper security and access to keep attacks at bay, but also through proactive risk detection and response.

Campus IT teams should craft strict policies and processes around data use and management, and include user education on AI tools in addition to institution-wide AI use policies and data governance.

"We used to be able to capture phishing attacks with e-mail by looking at the language, or seeing design errors, but that's no longer a viable clue or option," Kent said. "As AI has democratized, hackers can use it to launch attacks with greater efficacy as well as efficiency."

The baseline for establishing a secure AI environment should first tackle visibility, to gain understanding of where AI tools may already be in use by students, employees, and other systems shining a bright light on shadow AI. Additionally, an AI audit tool will show which AI companies like Meta, OpenAI, and DeepSeek are scraping and obtaining data from the universities' public-facing websites. As that information can be used to train those companies' large language models (LLMs), a university may no longer be credited for novel discoveries. Worse, sensitive or personally identifiable information (PII) may be put at risk.

Campus IT teams should craft strict policies and processes around data use and management, and include user education on AI tools in addition to institution-wide AI use policies and data governance. **Zero-trust access controls** are the order of the day to maintain and enforce appropriate data privacy and compliance with institutional as well as regulatory policies, lock down access to applications and systems, and ensure basic **data loss prevention**. Data management is critical for controlling data quality; that is, ensuring the appropriate data eventually feeds an institution's owned or developing AI/ML models, preventing hallucinations or bias in downstream outcomes.

Connect Securely, for Power and Collaboration

After the baseline is achieved, AI can be integrated more strategically, through applications like student-facing chat bots that can answer queries any time of day or night, or generative AI tools that help in research or provide IT teams efficiencies when writing code. AI can also be activated within existing tools. Institutions must focus tightly on data management, protection, and governance, ensuring proper labels, classifications and permissions are in place so AI tools and LLMs access only the data they should. Enhancing DLP and monitoring networks and applications continuously help institutions maintain compliance. API visibility and controls are also essential to ensure data remains secure as it flows from the cloud and/or an application to an AI tool or model.

"We recommend protecting the data exiting your environment through controls and tools like secure web gateway with DLP policies. In the AI world, we need to introduce new tools that control the traffic to and from the LLM. An AI gateway between the AI application and the model will provide visibility into what users are asking, and the response that flows back from the LLM, as well as which models they are leveraging" Kent said." For those building language models, data integrity is critical and using an AI firewall can protect the model from nefarious actors attempting to manipulate the data within."

A complete suite of SASE tools, including CASB, SWG, as well as access controls, ensures ongoing protection and visibility of data — all of which are essential before going all-in with AI and model development.

Accelerate Modernization and Efficiency

The operational efficiencies AI tools make possible — cost reductions and reduced complexities — couldn't come at a better time for higher education. In many ways, AI-enhanced solutions can speed up modernization projects, and help teams scale successful pilots campus- or institution-wide. And yet, shadow AI carries risks of hidden costs, Kent pointed out: "Beyond the security risk of shadow AI comes possible cost risks. Right now, transparency into the cost of leveraging models is weak, so AI users may not know exactly how much is the usage cost of leveraging the AI tool, especially if they are automating some of their processes. An AI gateway provides visibility into tool usage and can cache responses to control some of those costs."

A complete suite of SASE tools, including CASB, SWG, as well as access controls, ensures ongoing protection and visibility of data — all of which are essential before going all-in with AI and model development.

Build the Future

The next generation of AI/ML platforms and applications will be built by students and graduates who received a hands-on AI education on campus. Colleges and universities that stand up well protected and connected AI foundations open the door for more secure research and experimentation with AI/ML. Accessing scalable, composable, and responsive infrastructure that can accommodate new or growing models doesn't require massive upfront investment in on-premises or cloud-based servers. Cloudflare's **AI toolkit** provides infrastructure and access to open source models, LLMs, while enabling teams to build retrieval-augmented generation (**RAG**) AI applications, which ground foundation models to the data and information an institution controls beyond just data from the public web.

"Building applications of the future will mean integrating with AI, and our platform removes the complexity of managing infrastructure for the developer," Kent said. "When we talk about 'build,' that's our differentiator."

Protect data privacy and confidentiality

Defend against AI-powered cyber attacks

Maintain regulatory compliance

Cloudflare's connectivity cloud supports zero-trust security frameworks, application security, and data loss prevention solutions. **Discover more at cloudflare.com.**