Sponsored by

Spectrum BUSINESS®

5 Key Trends in Campus Technology

eCampus News

Technology is transforming all aspects of higher education operations, from teaching and research to managing facilities and ensuring the safety of students and employees. New innovations are making colleges and universities more efficient and are helping to drive student success.

However, a secure and reliable IT infrastructure is essential for delivering the kind of modern experiences today's students and employees require. To plan effectively for the future, campus leaders must understand the key trends and developments affecting their IT investments.

Here are five key trends every edtech leader should be aware of.

1. The rapid growth of AI is challenging campus administrators.

Artificial intelligence is altering teaching, learning, research and administration on college campuses at a head-spinning pace.

For instructors, AI can be harnessed to meet students' academic needs in real time, personalize the learning experience, create better learning tools, help in course design and development, streamline assessment and improve accessibility, such as by providing real-time translation services and multilingual support.

For campus leaders, AI can improve student recruitment by helping admissions offices target prospective students more effectively. It can also aid in retention by providing personalized tutoring and support for students, assist in academic and career advising, offer mental health support at scale, provide help desk and technical assistance and reduce administrative burdens by automating mundane or repetitive tasks.

For researchers, AI can help analyze massive datasets, develop new and better research models and accelerate the research process. For instance, AI can analyze terabytes of information and quickly identify patterns, saving researchers valuable time in their work.

But AI brings numerous challenges as well as benefits. Instructors are concerned about students using generative AI as a replacement for original work on assignments. Many colleges and universities still don't have up-to-date policies for students and faculty on how to use AI ethically and responsibly.

"Every student who graduates from a higher-ed institution should have at least one core course in AI or significant exposure to AI tools," Ravi Pendse, vice president for information technology and chief information officer at the University of Michigan, told *Inside Higher Ed*. "We will be doing a disservice to our students if we do not provide opportunities [for them] to acquire these skill sets."[1]

A 2024 EDUCAUSE survey revealed that colleges and universities are still looking for common ground on how AI should — and should not — be used for learning and work.

> "Every student who graduates from a higher-ed institution should have at least one core course in AI or significant exposure to AI tools."
>
> — Ravi Pendse, vice president for information technology and chief information officer, University of Michigan

Most respondents see a future in which AI tools are used for learning analytics (69%) and to improve accessibility for students (68%) and for faculty and staff (66%). Still, just under half of respondents (49%) disagreed that their institution has adequate resources and knowledge to support students with disabilities in using AI tools effectively. Respondents also worry that academic dishonesty will increase (64%) and that students will trust AI tools too much (60%).[2]

As AI tools continue to proliferate, campus leaders will have to answer many important questions, such as what limits they should put on AI use and how to educate their communities.

2. Campus networks must keep up with rising bandwidth requirements.

The surge in AI use on campus adds urgency to the need for secure, fast, and reliable network infrastructure that can scale easily to meet emerging needs.

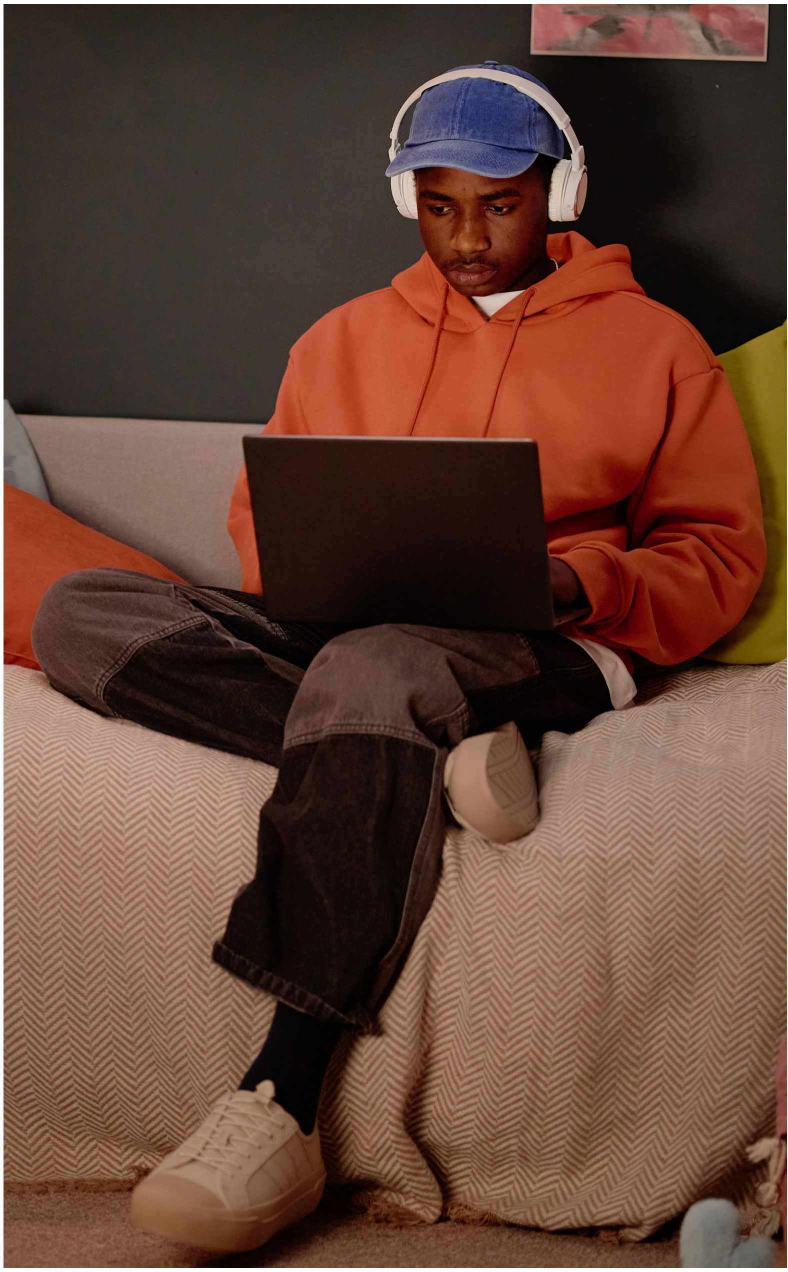
AI typically requires significant computing resources and near-instantaneous responsiveness. Technology analysis firm Omdia predicts that by 2030, nearly 75% of network traffic will involve AI content generation, curation or processing.[3] This can only be accomplished with fast, reliable and scalable networks.

But AI isn't the only application putting a strain on campus networks. Remote and hybrid learning environments are here to stay, with many students appreciating the opportunity to learn remotely. Many employees also continue to work remotely; in fact, 63% of administrative leaders and 51% of faculty members in a recent survey said that they were operating in a hybrid work environment.[4] These hybrid learning and working arrangements put a greater emphasis on network modernization, as colleges and universities must accommodate users both on and off campus.

What's more, the sheer number of devices interacting with campus networks continues to soar. Streaming video and gaming in residence halls; wearable technologies such as smart watches and fitness trackers; smart sensors, cameras and other Internet of Things devices — the list goes on.

To support the ever-increasing need for bandwidth, it's not uncommon for modern campus networks to exceed 100 gigabits per second of throughput. Recently, for instance, a public university in Florida upgraded its research network to provide up to 200 Gbps of throughput, while the rest of the campus has up to 20 Gbps.[5]

Modern, high-performance campus networks must meet certain criteria to ensure satisfaction among students, faculty and staff. They must be secure, reliable, responsive, robust and scalable. They must be flexible and adaptable, capable of expanding easily to accommodate new demands. And they must be built with intelligent technologies that can respond dynamically to users' needs, such as wireless infrastructure that can transfer users to access points with less of a load automatically.



3. Cybersecurity continues to be a top IT priority.

Cybersecurity is still a top-of-mind issue for IT leaders at colleges and universities of all sizes, and for good reason: From 2023 to 2024, there was a 25% increase in cyberattacks in the education sector, Zscaler reports.[6]

"As ransomware groups continue to target the sector with more sophisticated attacks — by leveraging tools like generative artificial intelligence — the potential impacts could be devastating. Institutions have no choice but to stay prepared and prioritize improving their security posture," says Hansang Bae, public sector chief technology officer for Zscaler.[7]

In April 2024, a New Mexico university was forced to cancel classes and had its payroll systems disrupted in a ransomware attack.[8] In September 2024, cybercriminals stole the sensitive health information of 1.47 million patients at a university Health Sciences Center and made it available online.[9]

But it's not just data breaches and ransomware that campus leaders need to worry about. Distributed denial of service (DDoS) attacks continues to be a problem as well. These brute-force attacks aim to overwhelm campus networks with more traffic than they can handle, thereby crippling the network. The disruption to services from DDoS attacks can be devastating.

While cybersecurity threats have only intensified in both frequency and nature, many organizations find themselves shorthanded in trying to respond. Nearly two in five IT leaders (38%) said their organization lacks sufficient understanding of staffing needs around cybersecurity, according to the "2024 CDW Cybersecurity Research Report." Only 10% of respondents considered themselves fully staffed.[10]

Colleges and universities need a multilayered approach to ensure protection from today's cyberthreats, such as a firewall service to protect the internet gateway, antivirus and anti-malware software to shield network endpoints, DDoS protection to guard against a distributed denial of service attack and so on. These multiple defenses all work together to enhance security by protecting against numerous types of threats, as well as multipronged attacks that seek to gain network access through multiple channels.

"From 2023 to 2024, there was a 25% increase in cyberattacks in the education sector."
— Zscaler ThreatLabz 2024 Ransomware Report

4. Zero trust has become a key cyber defense strategy.

A cybersecurity strategy that has become increasingly popular across all sectors is the concept of "zero trust." The idea is simple: Never trust — and always verify — each user, device and transaction, both inside and outside the organization.

A zero-trust approach acknowledges there's no longer a traditional network perimeter to be defended, because applications now reside in the cloud and users access the network from any location. In effect, the network edge extends to each individual user, and security is achieved by authenticating users' identities.

Zero trust requires a shift in mindset. Traditionally, once users have logged onto a campus network and been authenticated, they've had free range to explore and access basic resources. The assumption was that anyone allowed on the network belonged there and was trusted to move around freely.

Zero trust removes this assumption. With a zero-trust approach, all network users — wherever they're physically located — are *continuously* validated before being granted access to data and applications. To use the analogy of a castle, instead of being able to roam freely once they're inside the castle walls, users are stopped and asked to show their ID before entering every room.

Interest in zero trust has skyrocketed in recent years. In fact, a recent Gartner survey revealed that 63% of organizations worldwide have adopted a zero-trust stance.[11]

To implement this approach, colleges and universities need strong identity and access management tools in place to verify users' credentials. IT employees must be able to know who's on the network at all times, which applications they're using and how they're connecting. Campus networks must be finely segmented, and permission to access various types of resources should depend on factors such as the user's role, device, location and the data or application that is being requested.

A cybersecurity strategy that has become increasingly popular across all sectors is the concept of "zero trust." **The idea is simple: Never trust — and always verify** — each user, device and transaction, both inside and outside the organization.

5. Shifting from CapEx to OpEx models helps universities achieve predictable costs.

Traditionally, campus IT departments have purchased and installed network technologies through large capital expenditures. But the downside to this approach is that strategic IT planning is contingent on the availability of new funding. As a result, institutions might be stuck with outdated equipment until they can raise the capital they need for a network refresh cycle.

Shifting from a capital expenditures (CapEx) model to an operating expenses (OpEx) model, such as managed network services, can help colleges and universities solve this challenge. With a managed solution, rather than purchasing and owning network components, institutions instead would pay for network installation, upgrades, maintenance and repairs as a monthly service, like a utility.

A managed services approach can support more stable and consistent IT budgeting through an OpEx model. This helps leaders successfully predict and manage their network expenses, including the cost of routine maintenance. There are no longer any unpleasant surprises when a piece of equipment fails — and no more scrambling to find the money to replace an aging router or wireless access point.

Aside from more predictable costs, managed network services provide colleges and universities with knowledgeable experts who are available 24 hours a day, seven days a week to maintain, support, troubleshoot, upgrade and replace network infrastructure. This allows institutions to keep their networks running smoothly without having to commit their own IT personnel to the task. A managed services provider also ensures that firmware and security updates routinely occur across the network, keeping all systems continuously secure and up to date.

These are all key reasons why the number of organizations opting for managed network services is exploding. In fact, the global market for managed network services is expected to exceed $232 billion by 2037, a compound annual growth rate of more than 10%.[12]

A managed services approach can support more stable and consistent IT budgeting through an OpEx model. This helps leaders successfully predict and manage their network expenses, including the cost of routine maintenance.

Driving innovation

Edtech innovation isn't possible without a modern and flexible IT infrastructure that can support emerging technologies like AI effectively, keep up with rising bandwidth demands, secure data and applications with multilayered defenses and zero-trust capabilities and make budgeting easier with a shift to managed services.

Spectrum Business empowers colleges and universities to transform the student experience with networking, security, communications, collaboration and TV technology solutions. Our dedicated education IT experts serve hundreds of colleges and universities nationwide with a network engineered for exceptional performance, end-to-end accountability and 100% U.S.-based support, available 24/7/365.

Discover how **Spectrum Business** can help you modernize your IT infrastructure: **enterprise.spectrum.com/highered**

[1] Palmer, Kathryn. “How Will AI Influence Higher Ed in 2025?” *Inside Higher Ed*, December 19, 2024.
https://www.insidehighered.com/news/tech-innovation/artificial-intelligence/2024/12/19/how-will-ai-influence-higher-ed-2025

[2] Robert, Jenay. “2024 EDUCAUSE AI Landscape Study.” February 26. 2024.
https://www.educause.edu/ecar/research-publications/2024/2024-educause-ai-landscape-study/the-future-of-ai-in-higher-education

[3] Javaid, Usman, and Zerbib, Bruno. “AI needs a new networking core. Are we ready for it?” TM Forum, June 11, 2024.
https://inform.tmforum.org/features-and-opinion/ai-needs-a-new-networking-core-are-we-ready-for-it

[4] “Higher Ed’s Hybrid Workplace: How are colleges managing this new campus culture?” *The Chronicle of Higher Education*, 2023.
https://connect.chronicle.com/rs/931-EKA-218/images/RB_HybridWorkplace_Cisco.pdf?version=0

[5] Keller, Joel. “How to Future-Proof Your Higher Ed IT Infrastructure.” *EdTech Magazine*, September 25, 2024.
https://edtechmagazine.com/higher/article/2024/09/how-future-proof-your-higher-ed-it-infrastructure

[6] *Zscaler ThreatLabz 2024 Ransomware Report*.
https://www.zscaler.com/campaign/threatlabz-ransomware-report

[7] Kelly, Rhea. “2025 Cybersecurity Predictions for K-20 Education.” *Campus Technology*, January 30, 2025.
https://campustechnology.com/Articles/2025/01/30/2025-Cybersecurity-Predictions-for-K-20-Education.aspx

[8] O’Hara, Margaret. “Ransomware Attack Hits New Mexico Highlands University.” *Government Technology*, April 8, 2024.
https://www.govtech.com/education/higher-ed/ransomware-attack-hits-new-mexico-highlands-university

[9] Alder, Steve. “Texas Tech University Health Sciences Center Ransomware Attack Affects 1.46 Million Patients.” *The HIPAA Journal*, December 17, 2024.
https://www.hipaajournal.com/texas-tech-university-health-sciences-center-ransomware-data-breach/

[10] Stone, Adam. “Cybersecurity Automation Helps Short-Staffed Higher Ed IT Departments Protect Data.” *EdTech Magazine*, November 21, 2024.
https://edtechmagazine.com/higher/article/2024/11/cybersecurity-automation-helps-short-staffed-higher-ed-it-departments-protect-data

[11] “Gartner Survey Reveals 63% of Organizations Worldwide Have Implemented a Zero-Trust Strategy.” Gartner, April 22, 2024.
https://www.gartner.com/en/newsroom/press-releases/2024-04-22-gartner-survey-reveals-63-percent-of-organizations-worldwide-have-implemented-a-zero-trust-strategy

[12] “Managed Network Services Market Size & Share, by Component,” Research Nester, June 13, 2023.
https://www.researchnester.com/reports/managed-network-services-market/5013

eCampus News

This white paper was produced by **eCampus News**, the leading online platform that delivers daily technology news and information to higher-education administrators, educators, and technology professionals, and dedicated to the advancement and wise use of technology to improve teaching and learning for all. eCampus News offers ed-tech decision makers a wide range of informative content—including newsletters, webinars, case studies, white papers, websites, and more—that provide in-depth coverage of the latest innovations, trends, and real-world solutions impacting the education community.

www.eCampusNews.com

Spectrum BUSINESS®

Spectrum Business empowers colleges and universities to transform the student experience with networking, security, communications, collaboration and TV technology solutions. Our dedicated education IT experts serve hundreds of colleges and universities nationwide with a network engineered for exceptional performance, end-to-end accountability and 100% U.S.-based support, available 24/7/365.

enterprise.spectrum.com/highered