9 Smart Strategies to Help Secure Student Data in Higher Ed

On college tours, a beautiful campus and premium amenities can wow prospective students and their parents. Unfortunately, **an expansive IT campus ecosystem is just as enticing to cybercriminals**.

As higher education grapples with funding crunches alongside decentralized IT environments, limited staffing, and growing cyber threats, protecting priceless student information has never been more challenging—or more important.

These nine steps can help schools strengthen data security with modern, secure print and document workflows.

1

Move Toward Zero-Trust Architecture

A zero-trust model requires users to verify their identity continually. Multi-factor authentication (MFA), or using two or more credentials to access devices, helps prevent unauthorized access and bolsters a college's zero-trust posture.

While most universities already have MFA in place for their core systems, many fail to secure devices like printers, scanners, copiers, and multifunction devices (MFDs) properly, creating an easily exploitable gap. Cloud-connected print devices can be configured for MFA, creating consistent protection across every endpoint.

80% of higher education organizations have zero-trust strategies in place.[1]

2

Shrink Attack Surfaces

Departmental silos and bring-your-own-device (BYOD) cultures on campus create large attack surfaces with multiple entry points for hackers. That's why many CIOs are reducing their IT footprint by consolidating one-off devices like desktop inkjet printers and replacing them with cloud-connected network fleets. Doing so narrows potential points of compromise. It also reduces licensing and IT support costs.

3

Modernize Outdated Devices

Legacy printers and scanners bring multiple challenges. They often run on outdated firmware with known vulnerabilities that hackers can attack. Because they lack MFA capabilities, they can be accessed by anyone. And because they lack data encryption capabilities, scanned or printed documents can be easily intercepted. To help close these security gaps, IT directors should broaden their digital transformation efforts to include retiring legacy printers and embracing more modern solutions.

36% of higher education leaders list legacy IT systems as a top challenge.[2]

4

Secure Print Jobs

Some cybercrimes are decidedly low-tech. Consider a busy employee printing multiple documents from their desktop just before a critical meeting. In a rush, they grab a stack of papers off the printer but leave others behind. If those stray papers get into the wrong hands and they contain a student's social security number or a vendor's bank account information, that data is instantly compromised. Schools can avoid these scenarios with best-in-class devices that require badge access, so users must stand at the printer before releasing jobs.

5

Protect Scanned Documents

Scanned documents also open the door to multiple vulnerabilities. Data within digital files must be encrypted for full protection. Scanned documents also must comply with a university's retention policies. Switching to modern scanning technology with data encryption capabilities empowers educational institutions to digitize, classify, store, and retrieve information securely.

With such solutions, IT can encrypt set rules for the easy retrieval of scanned documents and improve information governance. They can also archive or dispose of outdated data in accordance with their retention schedules, supporting compliance initiatives. What's more, modern scanners can support master data management and enable the use of AI and machine learning to automate tasks and improve efficiency.

6

Expand Cybersecurity Awareness

Humans are the weakest link in any cybersecurity posture. Just one click of a compromised link by a student, faculty member, or staffer can open the door to stolen credentials or misdirected funds. Phishing campaigns like these are on the rise at U.S. universities, especially around key milestones like enrollment periods, financial aid deadlines, and tuition payment cycles.[3]

Schools can get ahead of these threats by instituting regular cybersecurity awareness and training. Unannounced phishing simulations, conducted via email, can teach users to identify and avoid phishing attempts and provide retraining whenever a user fails a test.

26% of all data breaches are caused by human error.[4]

Canon Managed Security Services combines awareness training with monitoring, threat detection, and remediation to strengthen campus security.

7

Centralize Visibility Across Devices

Mixed fleets of older and newer printers, scanners, and copiers can increase costs, cause technical issues, reduce efficiency, and make it impossible to monitor device use. Cloud-based platforms like uniFLOW Online from Canon can help schools integrate Canon and non-Canon printer fleets for added security and visibility.

With everything in one dashboard (logins, encryption, status, updates, and usage), IT doesn't have to hunt for information. Audit trails can simplify compliance, and the extra visibility makes it easier to catch unusual print activity and respond quickly.

8

Align Sustainability With IT Practices

Many of the same practices that protect sensitive student information also help institutions achieve their sustainability goals. Secure print release supports reduced paper waste. Network-connected devices help reduce energy use and lower the carbon footprint of legacy printers. And encryption features and audit trails help move schools toward higher levels of digitization. Centralized visibility helps IT teams monitor paper, ink, and supply usage, and can result in cost savings while promoting a more eco-friendly campus.

44% increase in donor requests about cybersecurity and sustainability strategies in 2024.[5]

9

Embrace Trusted Security Frameworks

Every new solution that colleges choose must be vetted fully for data protection capabilities. Trusted frameworks can help simplify decision-making for both IT and procurement leaders.

Solutions that align with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) follow guidelines and best practices for governing and protecting information.

Cloud services achieving Federal Risk and Authorization Management Program (FedRAMP) authorization provide standardized security assessments, helping to reduce duplicate testing and accelerate procurement.

Safeguard Student Privacy With The Support Of A Unified Approach

In the same way that it takes a village to educate a student, it takes a unified approach to keep sensitive student information safe. Consolidating multiple vendors into one contract can provide a secure, end-to-end, cloud-based digital workflow that helps to meet a university's printing needs and protects student data.

Canon offers an integrated ecosystem of technology (like uniFLOW Online), managed security services, and secure multifunction devices to help universities print securely, digitize smartly, and protect student data.

Explore how Canon supports student success in higher ed.

Sources:

[1] eCampus News, "Network Security in Higher Ed: The Importance of Zero Trust," July 2025.

[2] BDO, "2024 Nonprofit Standards Benchmarking–Higher Education Snapshot," October 2024.

[3] Doppel, "Social Engineering Tactics: Higher Education Phishing Attacks Surge," September 2025.

[4] IBM, "What Is a Data Breach?," May 2025.

[5] BDO, "2024 Nonprofit Standards Benchmarking – Higher Education Snapshot," October 2024.