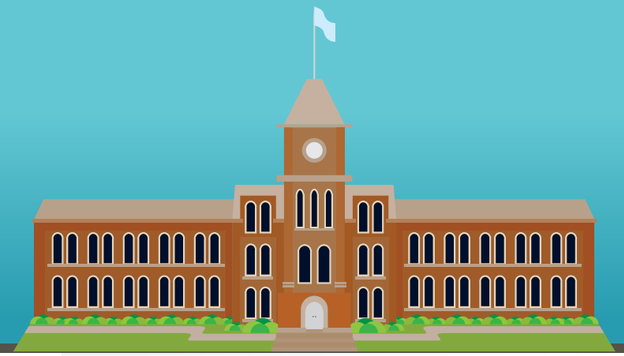
PROTECTING SENSITIVE STUDENT DATA AT THE PRINTER

As universities and colleges move toward digital communication and curriculum, they know they must protect online student data. But printed materials require the same level of security and attention. To fully protect student data, it's important to consider where and how information can be compromised.



KNOW THE LAWS

FERPA – The Family Educational Rights and Privacy Act prevents education institutions from sharing personally identifiable information (PII) from student records with third parties without written consent from parents and students.[1]

HIPAA – The Health Insurance Portability and Accountability Act prevents the disclosure of protected health information without an individual's authorization and provides individuals specific rights to their medical data.[2]

BEST PRACTICES AT A GLANCE

- Avoid printing PII, such as Social Security numbers, unnecessarily.
- Establish profiles to limit printer function access based on roles.
- Implement device authentication to release documents for print.
- Fax documents directly to emails, desktops and secure, in-printer storage.
- Protect printer hard drives with encryption, automatic deletion and overwrite capabilities.

RISK: When printing to off-site printers from mobile devices, papers left on output trays can expose sensitive data such as grades.

SOLUTION: By using a secure printing app and authentication codes at the printer, professors and faculty can worry less about confidential information being left on the output tray.

RISK: While working in communal spaces, students often print materials simultaneously, which can leave intellectual property and PII exposed.

SOLUTION: This risk can be reduced by requiring authentication at the printer, ensuring each student only prints and retrieves their documents.

RISK: Sending a fax containing sensitive health or financial information can put student data at risk.

SOLUTION: By faxing documents directly to a specified email account, desktop or secure storage within a designated printer, administrators can be more confident sensitive data will remain secure.

RISK: Documents sent to a server-connected printer are stored in the printer's hard drive, meaning any connected device is an open port for hackers.

SOLUTION: Automatic deletion, format overwriting, encryption and automatically created passwords help protect data transmitted to the device.

CENTER FOR DIGITAL EDUCATION

SPONSORED BY Canon CANON SOLUTIONS AMERICA

Canon Solutions America offers products, solutions, and services designed to help educators by streamlining manual processes, providing document security, reducing and controlling print expenses, and reducing the environmental impact of printing. To learn how Canon Solutions America can support your organization's document technology needs, please contact **1-844-50-CANON or visit csa.canon.com**.

1. http://ferpasherpa.org/s-p.html 2. www.astho.org/programs/preparedness/public-health-emergency-law/public-health-and-schools-toolkit/comparison-of-ferpa-and-hipaa-privacy-rule/