

FROM DEVICE TO DATA:

Creating an Efficient Workflow with Security in Mind in K-12 Education

K-12 school districts store massive amounts of sensitive data — including student grades, health records, and other personally identifiable information (PII). Due to this, they are a prime target for cyber attacks. K-12 institutions must also comply with various state and federal regulations, such as the Family Educational Rights and Privacy Act (FERPA), to protect student privacy. Many schools and districts lack a formal information policy, which can make data vulnerable.

THE AVERAGE COST OF A DATA BREACH IN EDUCATION IS \$4.77M*

THE AVERAGE COST PER RECORD IS \$142*

THE MAJORITY OF DATA BREACHES ARE FROM MALICIOUS ATTACKS: 51%*

THE AVERAGE TO IDENTIFY THE DATA BREACH IS 212 DAYS PLUS AN ADDITIONAL 71 DAYS TO CONTAIN IT.*

This infographic highlights some common areas of potential vulnerabilities in a typical K-12 digital workflow. It also shows the access controls and security features that can be layered on to help enhance document protection, increase efficiencies, and support compliance obligations — allowing K-12 schools and districts to focus on their core mission of improving student outcomes.



Layered Security

Layered security comprised of device security, print security, document security, information security, and cybersecurity, resulting in a comprehensive approach to protecting student information.

Automatic Alerts

An administrator can be alerted should someone attempt to print, scan, or copy sensitive documents that contain keywords (confidential, faculty only, etc.).

Defense at Device

Before accessing a device to print, scan, or copy, a teacher can use an authenticated ID card to help gain the appropriate level of access.

PII Protection

An administrator can print student grades from a mobile device, which are then held on a server with security features until he or she enters a password at a printer to retrieve them.

Compliance

A layered approach to protecting your organization can establish an effective security posture and thus facilitate compliance with regulatory guidelines.

Collaboration without Borders

When collaborating with staff and other departments, enterprise digital rights management (EDRM) tools enable administrators to control file level access to help ensure that information is not compromised.

PRODUCED BY

CENTER FOR
DIGITAL
EDUCATION

SPONSORED BY

Canon
CANON SOLUTIONS AMERICA

*2019 Cost of a Data Breach Study by the Ponemon Institute and IBM Security.

Canon U.S.A., Inc. and Canon Solutions America, Inc. do not provide legal counsel or regulatory compliance consultancy, including without limitation, Sarbanes-Oxley, HIPAA, GDPR, GLBA, Check 21 or the USA Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance. Canon products offer certain security features, yet many variables can impact the security of your devices and data. Canon does not warrant that use of its features will prevent security issues. Nothing herein should be construed as legal or regulatory advice concerning applicable laws; customers must have their own qualified counsel determine the feasibility of a solution as it relates to regulatory and statutory compliance. Some security features may impact functionality/performance; you may want to test these settings in your environment. Neither Canon Inc., Canon U.S.A., Inc. or Canon Solutions America, Inc. represents or warrant any third-party product or feature referenced hereunder. As of November 2019.
© 2019 CANON SOLUTIONS AMERICA, INC. ALL RIGHTS RESERVED.