IRONKEY™

ENCRYPTED USB STORAGE SOLUTIONS FOR EDUCATION

KINGSTON'S SECURE STORAGE

KNOW THE HIGH PRICE OF DATA BREACHES

From K-12 districts to four-year universities, educational institutions house volumes of personal information about students, faculty and staff. Credit card details, Social Security Numbers, grades and employment records — all can too easily fall into the wrong hands.

No wonder schools and other institutions must comply with regulations such as the Family Educational Rights and Privacy Act (FERPA) and the Payment Card Industry Data Security Standard (PCI DSS).

But when breaches do happen, the price can be high. Data breaches can trigger losses in research funding, threaten public-private partnerships, expose students and employees to identity theft, and deal serious blows to your reputation.

HOW DO YOU REIN IN A WIDE-OPEN ENVIRONMENT?

But education presents unique security challenges. Many institutions decentralize their IT operations across campuses or departments, and school-owned computers are physically available to dozens of people every day. Add mobility to the mix – with employees teleworking from home or other campuses, researchers moving from the lab to the field, and students bringing school computing home – and threats to your data, applications or networks multiply quickly.

COUNT ON KINGSTON TO KEEP DATA SAFE

With Kingston's encrypted USB drives which include industry favorites from Ironkey, you can simplify compliance by relying on a full range of products that include the right solution to meet every need. Kingston's encrypted line of drives feature products that range from Entry level Alphanumeric keypad PIN protection all the way through FIPS 140-2 Level 3* validated, military-grade encrypted USB storage devices. Kingston lets you put a wall between unauthorized users and the data you need to protect.

Choose from an array of Kingston IronKey and DataTraveler solutions:

- Hardware based encrypted USB flash drives
- FIPS Certification 197 through 140-2 Level 3 (Drive specific)

EASE THE BURDENS OF COMPLIANCE

Complying with FERPA, PCI DSS or GDPR requirements needn't be a burden. Use Kingston's managed USB drives seamlessly with the the DataLocker Ironkey EMS or Safeconsole Management products for advanced reporting and auditing capabilities to document how, where and when users have accessed, saved or modified confidential data.

GET THE KINGSTON ADVANTAGE

Mobilize faculty, staff, researchers and others by enabling them to safely access data and applications from virtually any PC.

Shield educational data with a virtually indestructible drive that exceeded military waterproof testing requirements.

Protect personal student and research data by putting military-grade encryption and a ruggedized enclosure between unauthorized users and your Kingston IronKey drive's contents.

Safeguard digital identities to prevent costly fraud or IP theft.

Comply with privacy regulations by relying on FIPS 140-2 Level 3* with advanced auditing and reporting.

Centrally manage data access and use, no matter where users go.

WITH KINGSTON SECURE STORAGE DRIVES...

- Faculty, staff and students can safely access data from home using virtually any PC or tablet.
- Researchers can update results at the lab, in the field, in an office, in the classroom or at home.
- Faculty can access institutional applications, data and more while attending conferences or symposiums.
- Administrators always have trusted access to data and applications.
- Adjunct faculty can securely work with institutional records and applications anywhere they have access to a any PC or tablet.
- Institutions can provide key personnel with critical data to maintain operations if severe weather or other disasters strike.
- IT can enforce access and use policies from a central console.
- IT can demonstrate best effort to comply with new and unsettled regulations, including the GDPR.

Kingston TECHNOLOGY