RISK & COMPLIANCE

Responsible Student Data Collection

A privacy policy can help ensure students' data is safe with your school — and build trust with parents.

Melissa Musser is director of risk advisory at Aronson LLC, an accounting and consulting firm. ***AronsonLLC.com***

Your school likely stores a vast amount of valuable student data, from attendance records to medical data. Parents and regulators have high expectations that you also take steps to safeguard this sensitive data, especially after the Facebook/Cambridge Analytica privacy scandal, in which 50 million user profiles were harvested, and in light of the E.U.'s new General Data Protection Regulation. To enhance trust, we recommend that schools develop and implement a data privacy policy, inform parents and faculty/staff about it, and closely evaluate the personal information your school collects and retains — and the personal information you really need to carry out the school's functions.

In short, a student data privacy policy helps schools responsibly collect data and maintain compliance with international, federal and state privacy laws. Generally it outlines why the school collects certain data and how it protects and disposes of it. Here are some helpful guideposts for crafting such a policy at your school (excerpted from the Generally Accepted Privacy Principles, developed by the American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants).

- **Management:** Define, document, communicate and assign accountability within the school for data privacy policy and procedures.
- **Collection:** Collect personal information only for the purposes identified in the policy.
- **Quality:** Maintain accurate, complete and relevant personal information.
- **Access:** Provide individuals with secure access to their personal information for review and updating.
- **Notice:** Notify individuals of the policy, and identify the purposes for which your school collects, uses, retains and discloses personal information.
- **Choice and consent:** Obtain implicit or explicit consent, and indicate individuals' choices with respect to the collection, use and disclosure of personal information.
- **Disclosure to third parties:** Disclose personal information to third parties only for clearly identified purposes and with consent.
- **Use, retention and disposal:** Limit the use of personal information to the purposes identified in the policy and for which the individual has provided implicit or explicit consent. Retain personal information only as long as necessary to fulfill the stated purposes or as required by law or regulations. Thereafter appropriately dispose of such information.
- **Security for privacy:** Protect personal information against unauthorized access, both IT and paper-based.
- **Monitoring and enforcement:** Monitor the school's compliance with the policy, and develop procedures to address privacy-related complaints and disputes.

PRIVACY RISK ASSESSMENT

In order to truly know where your school stands, we recommend performing a privacy risk assessment. Suggested steps:

- Classify information into general categories:
  - Personally identifiable/non-personally identifiable
  - Sensitive/non-sensitive
  - Subject to specific statutory/regulatory requirements
  - Medical
  - Financial
  - Collected from children
- Assess legal requirements domestically and abroad, in all relevant jurisdictions.
- Map data flows to provide detailed information about how the school receives, uses and manages information; the legal basis for processing information; and how the school passes information on to third parties.
- Determine how the school collects consent for different categories of information.
- Determine how the school stores, uses and destroys information.
- Determine to whom, under what circumstances, and in what manner the school may disclose information.

THIRD-PARTY RELATIONSHIPS

We also recommend that schools revisit existing agreements with vendors and other third parties. Do contracts include an expectation of privacy and data security measures, as well as limitations on liability in the event of mishandling or improper disclosure of sensitive data? If the third party is a technology company, inquire if the organization has signed the "Student Privacy Pledge," launched in 2014 by the Future of Privacy Forum and Software & Information Industry Association and signed by more than 300 companies. (See the pledge at left.) N

See this article on NetAssets.org for direct links to more information about student data privacy laws and policy recommendations.

The Student Privacy Pledge

is a list of 12 legally enforceable commitments that include not selling student personal information, and not collecting or using student personal information other than what is needed for the given educational purposes. Ed tech companies take the pledge to affirm they safeguard student data. The pledge concisely details existing federal law and regulatory guidance regarding the collection and handling of student data and encourages service providers to more clearly articulate these practices.

Learn more at ***studentprivacypledge.org.***