Safeguarding Student Data in Higher Education

DQC DATA QUALITY CAMPAIGN

Safeguarding student data is more than just a box checking exercise—it's a foundational part of effective data use. However, institutions of higher education often lack cohesive strategies for protecting student data at every level. By establishing data privacy as an institutionwide priority and setting shared expectations for faculty and staff, higher education leaders can ensure that student data remains secure and can be properly used to help students succeed.

Colleges, universities, and other institutions of higher education already collect a wealth of data on the students they serve. This information can provide critical insights into the paths students take through higher education and the supports they need to succeed, but it must be used **safely** and **effectively.** Robust data privacy practices prevent improper applications and disclosures of data, providing students with peace of mind that their personal information will remain private.

Data privacy is not the job of any one person. Everyone has a part to play in keeping student data safe and secure. While federal and state laws outline the data privacy requirements institutions must follow, administrators also have a broad purview over how their institutions approach implementing those requirements and safeguarding student data. They can lead the way on protecting student data by establishing privacy as a priority at every level of their institution and ensuring that their own data privacy policies are built upon a solid foundation of best practices. This brief presents three key ideas to consider when developing or refining data privacy policies and practices: **data governance, data protection procedures,** and **transparency.**

Higher Education and Privacy Laws

Institutions of higher education may be subject to a number of federal data privacy laws, including the following:

- **The Family Educational Rights and Privacy Act of 1974 (FERPA),** which regulates access to, amendment of, and disclosure of education records
- **The Gramm-Leach-Bliley Act and the Fair and Accurate Credit Transaction Act of 2003,** which govern how institutions collect, store, and use student financial information
- **The Health Insurance Portability and Accountability Act of 1996,** which governs how institutions protect student health records, including records kept by campus medical facilities
- **The Privacy Act of 1974,** which governs how federal agencies collect, use, transfer, and disclose student information

Additionally, state laws may affect how institutions collect, use, and share student data. Examples include the following:

- **Kansas's 2014 Student Data Privacy Act,** which builds on FERPA to ensure the privacy of student data for research
- **Texas's 2017 H.B. 2087,** which governs how institutions collect, use, and share student information on websites, online platforms, and mobile applications
- **Rhode Island's 2018 S.B. 2644,** which protects student data on school-owned or take-home technology

Student Data and COVID-19

The COVID-19 crisis sent shockwaves across the higher education landscape, forcing campuses to close their doors and quickly pivot to online learning. Many faculty and staff have tried to stay up to date on students' needs through online surveys, self-reported forms, and other informal data collections. The data they collect, as well as the data gathered through other COVID-related university programs and policies, potentially contains personally identifiable information or other sensitive details; however, it may fly under the radar of traditional data protection policies. Institution leaders and staff have a responsibility to ensure that all student data—including any COVID-related information—is subject to proper governance and data privacy policies.

Strong Data Governance Is the Foundation of Data Privacy

Data governance refers to the people, structures, and systems that shape how an institution handles student data. In colleges or universities, people need a place where they can come together to develop shared understandings of data privacy and make decisions. By establishing a sustainable forum dedicated to student data privacy, institution leaders ensure that they will be prepared to address evolving questions and concerns related to the collection, management, and disclosure of student data.

How can administrators use governance to address data privacy at their institutions?

- Establish **high-level leadership on data privacy.** Institutions may consider appointing an executive leader or oversight board who are focused solely on data privacy and are accountable for addressing current privacy priorities and adapting to future priorities. Representation from different colleges, departments, and offices in data leadership helps to ensure a shared understanding of data roles and responsibilities across every level of the institution.
- Clarify **data privacy roles and responsibilities.** All faculty and staff job descriptions should include descriptions of data-related roles and responsibilities, including how applicable data privacy laws might affect instructional practices. Institutions should also require new staff to participate in a data privacy orientation.
- Provide **ongoing professional development** on data privacy. Data governance bodies should develop trainings, workshops, and other learning opportunities that help all faculty and staff navigate new applications of privacy requirements, especially as evolving circumstances change established practices.
- Work with the right people to ensure that **vendors and contractors,** such as those providing online learning platforms, understand and adhere to the institution's data privacy policies and procedures. All contracts, data sharing agreements, and memoranda of understanding should reflect applicable data privacy laws and policies, articulate how each party is responsible for safeguarding student data, and include processes for monitoring compliance and handling incidents.

Data Protection Procedures and Policies Ensure That Student Data Is Safeguarded at Every Step

Data protection procedures and policies outline the specific ways institutions implement state and federal data privacy regulations and keep data safe through collection, use, and disclosure. With these procedures and policies in place, institutions can confidently use data to answer stakeholder questions, inform decisionmaking, and support students.

How can administrators implement data protection procedures at their institutions?

- Work with privacy experts to establish **comprehensive data privacy procedures.** These procedures should address how the institution maintains data privacy at every step of the process, as well as how the institution will monitor compliance and respond to privacy incidents. Broader changes to institutional programs or policies may have data implications; therefore, it is crucial that data privacy policies are updated to reflect current practices.
- Ensure that experts conduct **regular reviews** of the data privacy and security system. These reviews may include risk assessments, practice drills for privacy and security incidents, and security audits.
- Promote and uphold the **principles of minimal data use:** institutions should collect only the data that is absolutely necessary to fulfill a specific objective and no more. Through their data governance bodies, institutions should establish standardized processes for identifying the data that is necessary for a given purpose, as well as for proactively eliminating extraneous data collections.
- Establish systems for **documenting the universe of collected data.** Institutions gather large volumes of structured and unstructured data through various means (e.g., surveys, WiFi networks). The full scope of the collected data may not be widely understood by those within and outside of the institution. Maintaining an inventory of all data collections helps to uphold transparency and ensure that all student data is protected.
- **Talk to students** about what data the institution is collecting from them, how, and why. Students should also receive notice before their data is used in any new or different ways (e.g., new surveys) and have the chance to affirm or deny consent.

Transparency Is Critical to Maintaining Public Support for Data Use

Institutions promote transparency when they publicly share materials related to privacy policies and practices and establish clear internal and external communications policies. By sharing what steps they are taking to keep data safe and secure, institutions establish themselves as trusted data stewards.

How can administrators promote transparency at their institutions?

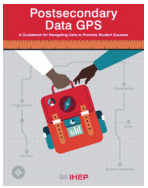
- Ensure that all policies and procedures related to how the institution collects, manages, discloses, and uses student data are **publicly available, clearly written, and easy to access.** These materials should be updated promptly following any changes to data policies or procedures.
- Appoint people responsible for **maintaining a public record of all data collections and all internal and external data requests.** This record should be easy for students and other interested parties to find and understand and should be updated regularly.
- Work with communications staff to provide **resources to the general public** explaining what data the institution collects, for what purposes, how it is protected, and students' rights over their data. Institutions may also develop tailored resources for specific stakeholder groups, such as students, staff, or researchers.
- When launching **a new data collection** (e.g., a student survey), communicate ahead of time to students and faculty about why the new collection is necessary, how the resulting data will be used, who will have access to it, and how it will be protected.
- As part of annual review processes, direct staff to **solicit broad public input** on improving data protection policies and procedures. Ensure that this process includes student voices, as well as those of faculty, staff, administrators, and other stakeholders.

Additional Resources

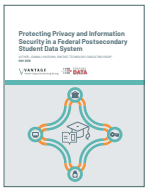
Complying with FERPA and Other Federal Privacy and Security Laws and Maximizing Appropriate Use. This brief from the Data Quality Campaign; EducationCounsel; and Nelson, Mullins, Riley, & Scarborough L.L.P. provides an overview of the state and federal laws that govern student data across early childhood, K–12, higher education, and the workforce.

The Emergence of Data Privacy Conversations and State Responses. This brief from the Institute for Higher Education Policy and the Data Quality Campaign addresses privacy considerations for linked state K–12 and postsecondary data systems.

"Information Security Guide: Effective Practices and Solutions for Higher Education." This resource from Educause provides practical guidance and tools on best practices in information security and privacy in higher education.



Postsecondary Data GPS: A Guidebook for Navigating to Promote Student Success. This resource from the Institute for Higher Education Policy outlines key questions, metrics, and other data considerations for institutions of higher education at every step in the postsecondary pipeline.



Protecting Privacy and Information Security in a Federal Postsecondary Student Data System. This brief from the Institute for Higher Education Policy and Vantage Technology Consulting Group outlines the federal laws and regulations that govern student data privacy for postsecondary institutions.

"Student Data Principles." Developed by a diverse coalition of national education organizations, this list of 10 principles provides a framework for effectively using and protecting student data.

"Student Privacy Compass." This web resource from the Future of Privacy Forum serves as a "one-stop shop" for finding information, news, and other resources related to student data privacy.

The Data Quality Campaign would like to thank José Luis Cruz, executive vice chancellor and university provost, and Jonathon Gagliardi, assistant vice chancellor for academic effectiveness and innovation, at The City University of New York for their advisement on the context of this brief.

DQC DATA QUALITY CAMPAIGN

The Data Quality Campaign is a nonprofit policy and advocacy organization leading the effort to bring every part of the education community together to empower educators, families, and policymakers with quality information to make decisions that ensure that students excel. For more information, go to www.dataqualitycampaign.org and follow us on Facebook and Twitter (@EdDataCampaign).