POLICIES FOR USERS OF STUDENT DATA:
A CHECKLIST

Privacy Technical Assistance Center

This Privacy Technical Assistance Center (PTAC) document aims to assist schools and districts in crafting data use policies to ensure appropriate protection of students' data. While it is not mandatory to develop a data use policy, the U.S. Department of Education recommends doing so as a best practice.

What is a data use policy?

Data use policies outline acceptable and prohibited activities for all categories of authorized data users (teachers, administrators, researchers, etc.). Effective policies clarify acceptable data use, define staff access, and outline compliance monitoring procedures along with consequences for noncompliance.

A data use policy is different from the policies that districts and schools typically develop to define acceptable student behavior online. Both types of policies are needed; students need guidance on appropriate and safe online behavior, and districts and schools need to regulate their use of student data.

Why should schools and districts have student data use policies?

From detailed records in student information systems, to personally identifiable information (PII) in online software used by teachers to enhance learning, to de-identified data provided to researchers for evaluating educational programs, students' personal information is collected and stored in many forms. Without the necessary data governance policies for all users of student data (see the PTAC document on Data Governance and Stewardship), the privacy and confidentiality of that information is at risk, leaving agencies exposed to complaints and investigations. While the Family Educational Rights and Privacy Act (FERPA) does not require a policy to be in place, it is a best practice to do so. Often districts develop data use policies for their schools, while occasionally individual schools develop these policies.

Best Practices

✓ Prepare data access and use policies for:

- Authorized user groups, such as teachers, administrators, IT staff, and researchers. Policies should acknowledge the differentiated access and responsibilities for each group.
- Device types, such as desktop machines, portable memory devices, district-issued mobile devices, and the users' own devices that access student data in any system. These include district-owned devices and those owned and operated by third parties on behalf of the school district.

Best Practices (cont.)

- ✓ A data use policy should include information on:
  - Acceptable and prohibited data use and related online activities.
    - Clarify acceptable and prohibited use for the various types of student data, such as student directory information, PII, and de-identified data.
    - Provide examples of permitted and prohibited uses and activities. Consider including "use cases" to illustrate complex scenarios.
    - Institute role-based permissions by job function so users may only access necessary student data; specifically prohibit data "browsing."
  - Acquisition and use of third-party apps and services that use student data in any capacity. If only specific programs or apps are approved for school and teacher use, make that list widely available.
  - Plans for monitoring policy compliance (e.g., passive network monitoring, regular audits of access logs, etc.).
  - Clear and enforceable consequences for non-compliance.
  - Information on legal protections that may apply to the students' data.
    - Federal laws, such as the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), and the Confidentiality Provisions in the Individuals with Disabilities Education Act (IDEA) protect students' education records and personal information.
    - Other federal, state, or local laws may apply as well. Consult your legal counsel about any other laws that may extend additional student privacy protections.
- ✓ Keep the policy as short and simple as possible to ensure users can recognize any violation. Use clear language and define legal and technical terms.
- ✓ Require a documented acknowledgement to access student data. Even if such an acknowledgement is not legally required, it is a best practice to have staff with access to students' PII acknowledge the district policies guiding student data use.
- ✓ Periodically review your data use policy, updating it as needed in response to changes in laws, regulations, software, or hardware.
- ✓ Regularly train staff on data use policies. These trainings could be paired with other trainings or offered ad hoc, but everyone with access to students' PII should be regularly reminded of their responsibilities with respect to this information.
- ✓ To promote transparency, post the policies online in an easily accessible location for staff to review as needed.

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about privacy, confidentiality, and security practices related to student-level longitudinal data systems. PTAC provides timely information and updated guidance on privacy, confidentiality, and security practices through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, confidentiality, and security of information in longitudinal data systems. Additional PTAC information and resources are available at http://ptac.ed.gov.