



Student **Data** Principles

10 Foundational Principles for Using and Safeguarding Students' Personal Information

High-quality education data are essential for improving students' achievement in school and preparing them for success in life. When effectively used, these data can empower educators, students, and families with the information they need to make decisions to help all learners succeed.

Everyone who uses student information has a responsibility to maintain the privacy and the security of students' data, especially when these data are personally identifiable. Meeting this responsibility starts with limiting the data that are collected, stored, shared, and used to support student learning and success. Whenever possible, aggregated, de-identified data that do not identify individual students should be used to inform key policy decisions and

help improve services and systems that benefit students. In instances where using personal information is necessary, those few individuals who have access to this information to carry out their duties must handle it in a legal, responsible, and ethical manner.

As organizations that believe passionately in the effective use of data to support student learning and success, we offer this set of principles for safeguarding students' personal information.

In addition to complying with federal, state, and local laws, we believe educational institutions and anyone who has access to students' personal information should adhere to and build upon the foundational principles on the back of this overview.

A coalition of national education organizations, representing a range of perspectives, experience, and stakeholders in the field, convened to develop these shared principles for safeguarding the personal information of America's students. See **www.studentdataprinciples.org** for a full list of supporters.

We believe:

- 1 Student data should be used to further and support student learning and success.
- 2 Student data are most powerful when used for continuous improvement and personalizing student learning.
- 3 Student data should be used as a tool for informing, engaging, and empowering students, families, teachers, and school system leaders.
- 4 Students, families, and educators should have timely access to information collected about the student.
- 5 Student data should be used to inform and not replace the professional judgment of educators.
- 6 Students' personal information should only be shared, under terms or agreement, with service providers for legitimate educational purposes; otherwise the consent to share must be given by a parent, guardian, or a student, if that student is over 18. School systems should have policies for overseeing this process, which include support and guidance for teachers.
- 7 Educational institutions, and their contracted service providers with access to student data, including researchers, should have clear, publicly available rules and guidelines for how they collect, use, safeguard, and destroy those data.
- 8 Educators and their contracted service providers should only have access to the minimum student data required to support student success.
- 9 Everyone who has access to students' personal information should be trained and know how to effectively and ethically use, protect, and secure it.
- 10 Any educational institution with the authority to collect and maintain student personal information should
 - a. have a system of governance that designates rules, procedures, and the individual or group responsible for decisionmaking regarding data collection, use, access, sharing, and security, and use of online educational programs;
 - b. have a policy for notification of any misuse or breach of information and available remedies;
 - c. maintain a security process that follows widely accepted industry best practices;
 - d. provide a designated place or contact where students and families can go to learn of their rights and have their questions about student data collection, use, and security answered.