NASBE
National Association of State Boards of Education

Student Data Privacy

Data is immensely valuable to education. Effective data use supports student achievement and allows the efficient operation of schools. However, data cannot be collected without factoring in the protection of that data. Safeguarding student privacy is a critical part of data use. Policymakers have a responsibility: to define how data is used by school officials (educators and staff), state and federal agencies, and third-party vendors who are working with schools; to inform families about their right to access and amend their child's data and know how that data is being used; and to safeguard the privacy, security, and accuracy of that data.

In order to ensure that state and local data collection is effective, secure, and protects individual rights, NASBE recommends that states create and/or supplement their state's privacy laws and policies with the following elements:

1 A statement of the purposes of the privacy law or policy that acknowledges both the educational value of data and the importance of protecting that data;

2 The designation of a person or group that is in charge of student data privacy for the state (which could be the state board of education and/or a newly created Chief Education Privacy Officer) that is responsible for: answering any stakeholder inquiries about student data privacy; and establishing and/or implementing statewide policies to protect all student data, including any collected post-secondary or workforce data, especially personally identifiable information;

3 A set of strategies for promoting transparency and public knowledge that makes information about the "who, what, where, why, and when" of data collection easily accessible to parents and the public clarifying the importance of data for educational purposes, how that data is being used and protected, and what their rights are to view and amend their child's data;

4 A provision limiting third-party vendors from using student data for non-educational purposes unless expressly authorized in writing by the school and allowed under federal and state law;

5 A review of the state's current resources related to student data privacy, such as

the state's staff and technical capacity to store, manage, and protect the data;

6 The creation of minimum statewide data security standards that incorporates administrative, physical, and technical safeguards; and

7 A plan for ensuring educators and administrators have the knowledge, skills, and support to use education data effectively and securely through methods such as teacher or administrator preparation programs, annual professional development, and evaluations of classroom data use and security on an ongoing basis.