National PTA
everychild.onevoice.

POSITION STATEMENT

STUDENT DATA PRIVACY AND SECURITY

National PTA and the students and families we represent understand the value of collecting student data to support educational outcomes. In a 2015 study, Parental Support for Technology and Data Use in Schools—conducted by the Future of Privacy Forum—parents indicated support for the access to, and use of, student data to improve teaching and learning. Yet parents articulated that there must be a clear justification for the need and benefit to access and use their child's data in educational settings. Despite support for the use of student data, parents are concerned about the privacy and security of their child's personally identifiable information and educational record.

National PTA is deeply committed to the promotion of privacy and security policies that maintain the confidentiality of sensitive data that students and families provide to educational institutions, as well as the data that is collected while using online products and services.

In 1974, the passage of the Family Educational Rights and Privacy Act (FERPA) ushered in a new era in federal educational privacy rights through its application of fair information practices to educational records. FERPA has provided individuals—or their parents in the case of minors prior to enrollment at postsecondary institutions—with the right to inspect and review their educational records, exercise significant control over the disclosure of information from those records and correct or amend erroneous information in the records. The regulations included several "fair information practices" to provide for these rights such as notice and review and the right to control redisclosure of a student's educational record.

In 1998, Congress passed the Children's Online Privacy Protection Act (COPPA) to protect the privacy of children under age 13 when using commercial websites and online services, including mobile apps. The primary goal of COPPA is to ensure parents are in control over what information is collected when their young children are online.

Current federal laws do not contemplate electronic records, online service provider rights and responsibilities or individual electronic student profiles. Therefore, federal laws such as FERPA and COPPA must be modernized to better protect student's educational records and the collection of information gathered online to address the growing use of technology and data in education and throughout society. Congress must also address the emerging use of service providers who provide online educational resources and tools for children, families and schools to ensure there are adequate parameters around the collection, storage, security and destruction of a child's or student's personally identifiable information and/or educational record.

National PTA supports the ability of families and students to have reasonable control over the collection, warehousing and use of electronic student data, while also supporting the need for research and data analysis to improve student learning outcomes, instructional design and

remedial supports. Additionally, National PTA supports current federal law (COPPA) that requires direct notice to parents and parental consent before an operator collects personally identifiable information and that privacy policies must be clear and accessible to families.

National PTA opposes the wholesale data-mining of educational records or online profiles for unspecified and open-ended purposes. The association recognizes educational agencies and institutions as the nexus between parents seeking access to their child's data and the service providers that collect the data within a school setting. In managing this relationship, educational agencies should balance parental rights with educationally sound data uses, like personalized and adaptive learning.

To that end, National PTA recognizes the important role parents and families play as partners in protecting and ensuring the security of student data. The association and its constituent bodies promote the establishment of and support for policies and procedures that:

- Inform parents and families on the relevant federal, state, tribal and local laws on student data privacy and security, including consent and notification provisions
- Require states, school districts and schools to be transparent and engaged with families on the development, implementation and notification about policies and procedures related to the privacy and protection of student data in accordance with state and federal privacy laws, including educating students on their right to privacy
- Allow for parents and families to retain the right to review, inspect and obtain copies of their child(ren)'s education records or online profiles and request corrections to inaccurate digital or hard-copy information
- Ensure student data is used for authorized educational purposes only; and prohibit the sale of student data, and/or its use to target non-education related advertising to students and their families
- Ensure school districts and online service providers' privacy and security policies are clear, easy to read and accessible to all parents and families
- Require school districts to designate a privacy and security officer to ensure compliance with privacy law and coordinate the necessary professional development for teachers, principals and any school employee or official who handles student data
- Require school districts and schools to annually (at a minimum) provide teachers, principals and any school employee or official who handles student data with the appropriate professional development to ensure proper privacy and security for student data
- Require school districts and online service providers to have reasonable policies and procedures in place to effectively and appropriately handle data breaches, including

procedures to notify students and families, and notification to affected educational institutions in the case of an online service provider breach

- Require online service providers to have a comprehensive protocol to ensure the privacy and safety of student data—that includes the collection, storage, dissemination and cyclic destruction of stale student data
- Require contracts between school districts and online service providers to provide for the ownership of student data upon dissolution of service; provide for the safe keeping of student data after the service relationship has ended and permit the use of student data only in ways necessary to fulfill the contract with the school or district

Adopted: by the 2015 Board of Directors