Our Commitment to Parents: Clear Data Privacy Practices @ ACES

Brought to you by the ACES Data Privacy Team and the ACES Internal Technology Committee (AITC)

WHY?

Parents and guardians want assurances that personal information and data about their children are secured and protected by ACES. These questions are rising as we use the Internet, mobile apps, cloud computing, online learning, and new technologies to deliver exciting new education and health services. At ACES, we strive to be clear about what data we collect, how data support a child's education, and the safeguards in place to protect that data.

WHAT data do we collect?

Operating Schools

We collect data such as addresses, phone numbers, gender, and age, as well as, health information to ensure student safety and accurate reporting to help run our operations efficiently.

Measuring Progress of our Students and Clients

We collect data such as attendance, grades, and participation in school activities to enable students to succeed.

Improving the Education Program

We collect results and content from local, state, and national assessments to provide teachers, administrators, parents, state, and federal agencies important information about student, program, and school performance.

Striving to Meet the Needs of Students

We collect surveys and other feedback to improve teaching and learning.

HOW does education data support student success and school improvement?

Data = Success!			
TEACHERS need data to understand when students are thriving and when they need more support in learning specific concepts.	PARENTS and guardians need access to their child's educational data to help them succeed.	STUDENTS need feedback on their progress so they can make good decisions about program choices and prepare for success.	SCHOOL OFFICIALS and stakeholders need to understand school performance and know if scarce education resources are being allocated effectively.

Our commitment

We are working to improve your children's education by ensuring it meets their unique needs. It would be very difficult to accomplish this goal without the ability to capture important information about your child's progress. Protecting personal and health information in secure and responsible ways is at the heart of our efforts to provide a richer, dynamic, and personalized learning experience for all learners at ACES. Please visit our data privacy web portal for more information and a current list of applications used at ACES: http://www.aces.org/administration/curriculum-programs/educational-technology/data-privacy-practices/

Our Commitment to Parents: Clear Data Privacy Practices @ ACES

Brought to you by the ACES Data Privacy Team and the ACES Internal Technology Committee (AITC)

HOW is education data protected?

ACES follows federal and state education privacy laws and adheres to privacy, health, and security policies. When we use an online service provider to process or store data, that provider must adhere to federal and state privacy laws including current security protocols and technology.

The federal Family Education Rights & Privacy Act (**FERPA**) gives parents rights related to their children's education records and personally identifiable information (PII). Parents may opt-out of releasing their child's information for marketing, including yearbooks. Parents have a right to inspect their child's educational record. Annually, ACES will notify parents of the vendors of software, applications, or apps (fee-based or free). For more information, visit https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html	The federal Health Insurance and Accountability Act of 1996 (**HIPAA**) regulates the protection of privacy and security of certain personal health information (PHI). As a covered entity, ACES follows all HIPAA requirements for safe usage and secure storage of both PII and PHI data of staff and students. For more information, visit https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html	The federal Children's Online Privacy Protection Act (**COPPA**) prevents child-directed websites and apps from collecting certain personal information from anyone under 13 years of age without parental permission. Our school system may consent on behalf of parents in the education context when student information is collected for the school's exclusive use and benefit and for no other commercial purpose. For more information, visit https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule	The federal Children's Internet Protection Act (**CIPA**) addresses concerns regarding children's access to obscene or harmful content over the Internet (e.g., filters and education). CIPA imposes requirements for educating students and staff in digital citizenship (including interacting on social networks and cyberbullying). This requirement is a prerequisite to receive federal and state funding, such as the federal E-rate program. For more information, visit https://www.fcc.gov/consumers/guides/childrens-internet-protection-act	The federal Protection of Pupil Rights Amendment (**PPRA**) and the **Connecticut State Student Data Privacy Act** dovetail with FERPA and COPPA. Any vendor of software, websites, or applications (fee-based or free) must sign a contract agreeing to the conditions of the law. ACES notifies parents of screened vendors through the ACES website at https://www.aces.org/schools-programs/school-based-services/educational-technology/data-privacy-practices. The website includes our processes, contracts, parent exemptions, breach notifications. For more information, visit the PPRA site at https://www2.ed.gov/policy/gen/guid/fpco/ppra/parents.html and the CT updated House Bill for student data privacy at https://www.cga.ct.gov/2018/ACT/pa/pdf/2018PA-00125-R00HB-05444-PA.pdf

Reference: Information adapted from the COSN (2015). Protecting privacy in connected learning toolkit. Retrieved from http://www.cosn.org