

# Clear Data Privacy Practices for Staff @ ACES

Brought to you by the ACES Student 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 secure 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 services.<sup>1</sup> 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. The new CT law on student data privacy (HB 5469 PA 16-189) dovetails with existing federal laws (COPPA, CIPA, FERPA, and PPRA - *see flip-side of this flyer*).

## WHAT is new about the CT Act Concerning Student Data Privacy (HB 5469 PA 16-189)?

<p><b>Overview</b></p> <p>As of October 1, 2016, this act restricts how student information may be used by contactors and 3<sup>rd</sup> party operators of websites, online services, and mobile applications. In addition it requires parent notification of contracts, approved sites, and security breaches. The act applies to free and paid services.</p>	<p><b>Contractors &amp; Operators</b></p> <p><b>Contractors</b> and <b>Operators</b> of websites and apps that use student information are required to sign contracts with ACES to operate and use ACES student information with new privacy restrictions (e.g., PowerSchool, Google, Canvas, iReady, Khan Academy).</p>	<p><b>Transparent Approval Process</b></p> <p><b>ACES must post on our external website our policy, process, and contracts for <u>online services using student information</u>.</b></p> <p><b>The approval process by AITC includes three stages:</b></p> <ul style="list-style-type: none"> <li>➤ <b>Inventory resources;</b></li> <li>➤ <b>Privacy review and contracts; and</b></li> <li>➤ <b>Curriculum and technology review.</b></li> </ul>	<p><b>Parent Notifications – Privacy and Security</b></p> <p>Notifications on ACES website:</p> <ul style="list-style-type: none"> <li>➤ Policy and processes,</li> <li>➤ New contracts, and</li> <li>➤ Websites approved by ACES.</li> </ul> <p>Notifications on website within 2 business days:</p> <ul style="list-style-type: none"> <li>➤ Breaches of student information.</li> </ul>
---	--	--	--

## HOW does this LAW affect all ACES staff? WHAT can you do?

Using and protecting personal 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.

<p><b>Privacy</b></p> <p>BEFORE clicking AGREE to use any online application, service, or resource ask:</p> <ul style="list-style-type: none"> <li>➤ Does the resource use student information (e.g., logins, names)?</li> <li>➤ If yes, <a href="#">check the approved resource list</a>. If it is listed as approved, you may use the tool.</li> <li>➤ If the product is not listed, <a href="#">request a review</a> from AITC to initiate the <a href="#">process</a>.</li> </ul>	<p><b>Security</b></p> <p>Breaches may happen through vendor, technology, or human error. Human error represents 95% of data breaches<sup>ii</sup>.</p> <ul style="list-style-type: none"> <li>➤ Do not send or share student data with anyone that does not have a legitimate educational need for it. Use permissions to secure files.</li> <li>➤ Use only secure resources to store information about students (e.g., interACES, PowerSchool, IEP Direct). These resources do not allow student access, therefore eliminating the human error of giving permission for students to view by accident.</li> <li>➤ Do not use thumb drives, external drives, or desktops. They are easy to lose and put data at risk. If you lose a device with student information, contact your administrator and email <a href="mailto:ACESBreachNotice@aces.org">ACESBreachNotice@aces.org</a></li> <li>➤ Change your passwords often and avoid using generic or easy to guess passwords.</li> <li>➤ Be careful about putting student data in emails. Use initials only. Emails are part of the educational record and may be requested through FOIA.</li> <li>➤ Do not leave your computer logged in when not in use.</li> <li>➤ <b>Please email <a href="mailto:ACESBreachNotice@aces.org">ACESBreachNotice@aces.org</a> IMMEDIATELY of any breaches.</b></li> </ul>
---	--

Check Status

Request Review

Review Process

Parent Portal

# Clear Data Privacy Practices for Staff @ ACES

Brought to you by the ACES Student 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 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>

Additionally, 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. Starting October 1, 2016, any contractor of software, applications, or apps (fee-based or free) must sign a contract agreeing to the conditions of the new law. Operators of websites must provide privacy policies compliant with the law. ACES will notify parents of screened vendors through the ACES website. The website includes our policy, processes, ongoing additions, changes, copy of contracts, and notification of breaches. For more information, visit 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>

## Questions and suggestions?

ACES Student Data Privacy Team: [Tim Howes](#), [Vanessa Taragowski](#), and [Wanda Wagner](#).

ACES Internal Technology Committee (AITC): [ACESAITC@aces.org](mailto:ACESAITC@aces.org)

<sup>i</sup> Information adapted from the COSN (2015). Protecting privacy in connected learning toolkit. Retrieved from <http://www.cosn.org>  
<sup>ii</sup> Howath, F. (2014). The role of human error in successful security attacks. Retrieved from <https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/>

