Clear Data Privacy Practices for Staff @ 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 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 and health services.[i] 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 CT law on student data privacy (HB 5469 PA 16-189) dovetails with existing federal laws (COPPA, CIPA, FERPA, PPRA, HIPAA - *see flip-side of this flyer*).

WHAT is new about personally identifiable information (PII) and personal health information (PHI)?

Overview

CT HB 5469 and PA16-189 restrict how student data may be used by contactors and 3rd party operators of websites, online services, and mobile applications. The act applies to free and paid services. In addition, as a covered entity under HIPAA, all ACES staff must follow both FERPA PII and HIPAA PHI compliance requirements.

Vendor Contracts

Contractors and operators of websites and apps that use student information are required to sign contracts with ACES to operate and use ACES student information with privacy restrictions (e.g., PowerSchool, Google, Canvas, iReady, Khan Academy).

Transparent Approval Process

ACES must post on our external website our policy, process, and contracts for online services using student information.

The approval process by AITC includes multiple stages: (a) inventory resources; (b) privacy review and contracts; (c) curriculum review; and (d) technology security review.

Parent Notifications – Privacy and Security

Notifications on ACES website:

- Policy and processes,
- New contracts, and
- Websites approved by ACES.

Notifications on website within 2 business days:

- Breaches of student and staff PII or PHI.

HOW do these laws affect all ACES staff? WHAT can you do?

Using and 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.

Privacy

BEFORE clicking AGREE to use any online application, service, or resource ask:

- Does the resource use student information (e.g., logins, names)?
- If yes, check the approved resource list. If it is listed as approved, you may use the tool.
- If the product is not listed, do not use and request a review from AITC to initiate the process.

Security

Breaches may happen through vendor, technology, or human error. Human error represents 95% of data breaches[ii].

- Do not send or share student data with anyone that does not have a legitimate educational need for it. Use permissions to secure files.
- Use only secure resources to store information about students (e.g., interfACES, PowerSchool, IEP Direct). These resources do not allow student access, therefore eliminating the human error of giving permission for students to view by accident.
- Do not use thumb drives, external drives, or desktops. They are easy to lose, put data at risk, and are not backed up. If you lose a device with student information, contact your administrator and email ACESBreachNotice@aces.org
- Change your passwords often and avoid using generic or easy to guess passwords.
- Be careful about putting student data in emails. Use initials only. Emails are part of the educational record and may be requested through FERPA or FOIA.
- Do not leave your computer logged in when not in use.
- When traveling with PII or PHI information, secure the documents in an HIPAA compliant locking bag.
- Check the parent portal: https://www.aces.org/schools-programs/school-based-services/educational-technology/data-privacy-practices

Clear Data Privacy Practices for Staff @ 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

Questions and suggestions? ACES Student Data Privacy Team: Tim Howes, Vanessa Taragowski, and Wanda Wagner. AITC: ACESAITC@aces.org

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

[ii] 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/