DATA PRIVACY AND SCHOOLS
Outlining the Conversation

TECHNOLOGY IN THE CLASSROOM: EXISTING SCHOOL DATA REGULATIONS

Schools are required to comply with a number of complex regulations related to data privacy and security. These include:

Children's Online Privacy Protection Act (COPPA) Obligations

In certain circumstances, schools may—if they choose—act as intermediaries between operators of websites or online services and parents in the notice and consent process. They may act in lieu of the parent in approving the collection of personal information from students under the age of 13 when the information is only used for the benefit of the school.

- If schools want to act in lieu of the parents in providing consent for collection of personal information from students, they must first assess how the operator of the website or online service will collect, use and disclose that information, and they must confirm that the data will not be used by the operator for any other commercial purpose.
  - Schools must assess the privacy policies and practices for each website and online service being considered for use in the classroom.
  - Schools are advised to keep their Acceptable Use Policy up-to-date when technology is added to the classroom.

Family Educational Rights and Privacy Act (FERPA) Obligations

Schools must give parents certain access to their children's education records. Classroom technology and data repository services may further complicate FERPA requirements for schools.

- Schools must determine whether or not a variety of third-party operators meet FERPA requirements for protecting student privacy with respect to data that is housed on their servers, applications, and software, and ensure that the operators are not accessing the data for other purposes.

- Schools may need to determine how to track data and progress reporting performed via technology used in the classroom, so that it may be made available to parents.
- Schools may need to determine how to provide parents with access to all student data they have stored on repository services.

Children's Internet Protection Act (CIPA)
Beyond blocking inappropriate material, schools and libraries must "adopt and implement an Internet safety policy that addresses," among other things "the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications" and "unauthorized disclosure, use, and dissemination of personal identification information regarding minors."

- As technology is added to the classroom or library, the products must be assessed in relation to existing safety policies, which may need to be modified accordingly.

Exploratory Questions

1. Are schools aware of their COPPA obligations?

2. To comply with COPPA and FERPA:
   - How can schools be equipped to assess privacy policies and practices of operators for the technology that might be used in the classroom?
   - How can schools be equipped to assess privacy policies and practices of vendors that might house and have access to student data?

3. How can schools be encouraged to share reporting with parents to better understand their children's progress, building a community of support—school, student, parent—focused around the child's academic success?

4. What are the potential FERPA implications related to disclosing a student's personally identifiable information to an operator of a website or online service when that information is only to be used for the benefit of the students and school system?
   - Do those FERPA obligations apply if the parent has provided the COPPA consent?

5. Teachers and school counselors are being asked to record behavioral characterizations and bullying incidents onto platforms where they might be shared with another school when a child transfers.
   - How are schools to balance these requirements with FERPA and COPPA rules (if combined with personal information)?

6. What are the COPPA and FERPA implications that schools must consider related to personally identifiable data that is captured by a platform, website, or app if that data is transmitted to a data repository?

7. How are schools tracking data collected by operators of technology used in the classroom?
   - Does such tracking result in maximal collection and storage of student data by the schools?

8. How are CIPA safety policies being assessed and updated in response to use of technology in the classroom and data repository services?

9. How are states helping school districts define and manage their data privacy practices?

10. Who are the stakeholders that can best inform models of in-school data management practices?