CoSN LEADING EDUCATION INNOVATION

Protecting Privacy in Connected Learning
A CoSN Leadership Initiative

Ten Steps Every District Should Take Today

With so much uncertainty about what districts can or should be doing to help protect the privacy of student data, it can be easy to lose sight of some very concrete steps that can be taken today.

1. **Designate a Privacy Official**—A senior district administrator needs to be designated as the person responsible for ensuring accountability for privacy laws and policies. The work of implementing and ensuring compliance must be collaborative, and will cut across many departments, but someone needs to be in charge.
2. **Seek Legal Counsel**—Make sure that the legal counsel used by your district has access to and understands education privacy laws and how they are applied to technology services. Do not wait until there is a pressing issue that needs to be addressed.
3. **Leverage Procurement**—Every bid or contract can include standard language around a wide range of legal issues. By adopting standard language related to privacy and security you will make your task much easier. However, many online services are offered via "click-wrap" agreements that are "take it or leave it." You may have to look for alternative solutions or negotiate a rider with the vendor if the privacy provisions of those services do not align with your expectations.
4. **Know the Laws**—Many organizations have published privacy guidance for schools, such as this Toolkit. The US Department of Education's Privacy Technical Assistance Center is a must-know resource at http://ptac.ed.gov/.
5. **Adopt School Community Norms & Policies**—Beyond the privacy laws, what does the school community really expect when it comes to privacy? Seek consensus regarding collecting, using and sharing student data.
6. **Implement Workable Processes**—There must be processes in place for selecting instructional apps and online services. No one wants to slow innovation, but ensuring privacy requires some planning and adherence to policies. Once enacted, the policies should be reviewed regularly to ensure that they are workable and that they reflect current interpretations of privacy laws.
7. **Provide Training**—Staff need training so they will know what to do to protect student data privacy and why it is important. Annual training should be required of any school employee that is handling student data, adopting online education apps and contracting with service Providers. Privacy laws represent legal requirements that need to be taken seriously.
8. **Inform Parents**—Parents should be involved in the development of privacy norms and policies. Just as schools provide information about online safety and appropriate use, they need to put significant effort into making sure that parents understand how schools use student data, and the measures taken to protect student privacy.
9. **Make Security a Priority**—Privacy and security go hand-in-hand. Secure the device, the network and the data center. Toughen password policies. Confirm that your data retention policies align with state legal requirements. Monitor your network for threats. Have regular security audits conducted by a third party expert.
10. **Review and Adjust**—Stay informed about guidance issued by ED and other regulatory authorities to help inform application of privacy laws, and about new laws that may be introduced. Keep your school policies and practices updated to reflect legal requirements and community norms.

Excerpted from Making Sense of Student Data Privacy (May 2014), authored by Bob Moore, Founder, RJM Strategies LLC and supported by Intel. The full report can be found at http://www.k12blueprint.com/privacy.