



Ten Steps Every District Should Take Today

With so much uncertainty about what districts can or should be doing to help ensure the privacy of student data, it would 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. This is a “divide and conquer” issue, but someone needs to be in-charge.
2. **Seek Legal Counsel**—Make sure that the legal counsel your district has access to 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. **Know the Laws**—Many organizations have and will be publishing privacy guidance for schools, such as the toolkit CoSN toolkit available at <http://www.cosn.org/privacy>. The US Department of Education’s Privacy Technical Assistance Center is a must-know resource at <http://ptac.ed.gov/>.
4. **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.
5. **Implement Workable Processes**—There must processes for selecting instructional apps and online services. No one wants to slow innovation, but ensuring privacy requires some planning and adherence to processes. Once enacted, the processes should be reviewed regularly to ensure that they are workable and that they reflect current interpretations of privacy laws and policies.
6. **Leverage Procurement**—Every bid or contract has 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. Unfortunately, many online services are offered via “click-wrap” agreements that are “take it or leave it.” You may have to look for alternatives solutions if the privacy provisions of those services do not align with your expectations.
7. **Provide Training**—Staff need training so they will know what to do or 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 the measures taken to protect student privacy.
9. **Make Security a Priority**—Privacy starts with security. Secure the device, the network and the data center. Toughen password policies. Have regular security audits conducted by a third party expert.
10. **Review and Adjust**—Interpretations of privacy laws are changing and new laws may be added. School policies and practices will need updating and adjusted so that they reflect legal requirements. Processes can become burdensome when that happens, some people may want to skirt the process.

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>.