New Challenges of Educational Technology for Washington Schools

BY CHARLES LEITCH, ESQ., CIPP/G, GUEST CONTRIBUTOR TO *POLICY & LEGAL NEWS**

[Editor's Note: WSSDA frequently receives requests for a model policy on Social Media. As Mr. Leitch explains in the following article, WSSDA continues to monitor the legal and legislative landscape of social media, but a statewide model, even when ripe, will be of limited use in this district-specific area of K-12 policy.]

WSSDA is charged with creation of model policies and procedures for all School Districts in the State of Washington. For particular areas such as student technology supervision and education, however, developing a scalable model policy for districts can be especially challenging. Technology deployments vary greatly from district to district and this can create policy and procedural challenges that can be daunting. In order to effectively develop and establish district-specific policies and related procedures, and to prepare for forthcoming expected mandates, it is imperative that each district establish true understanding of their technology infrastructure, staff skillset, supervisory practices, and student education efforts on technology and social media.

Establishing Knowledge Of Student Technology Use

Faced with limited resources and available staff, it is no surprise that some districts lack centralized administrative understanding of how students are allowed access to technology (and therefore social media) within each school in and out of instructional time, or how students are supervised and educated on appropriate use. Such an effort is suggested to assist in assessment and clarification of technology goals and policy development. Such an inventory of supervision and instruction, when consolidated, also serves to focus all school site administrators on a common baseline.

Inconsistent Device Regulation

Under RCW 28A.320.135, district boards may adopt policies that limit the possession of telecommunication devices, including cellular phones, by students that deliver communication to the possessor. In practice, the determination of use rules is left to each school site. This however has led to variance between schools in the same district and oftentimes inconsistent messaging with students as to expectations. Consistent regulation is reasonably construed as a healthy component of a positive school climate and clear notice of expectation to all students as well as staff.

E-Rate Compliance Issues

Since its passage in 2001, the Children's Internet Protection Act (CIPA) requires schools to certify that they have in place certain internet safety policies and technology protection measures to receive "E-Rate" funding to support affordable telecommunications and internet access. One of the significant requirements is protecting minors from accessing visual depictions of obscenity, child pornography, or harmful material via the internet. As a result, public schools in the United States started blocking access to many internet sites.

(continued)

> **“Technology deployments vary greatly from district to district and this can create policy and procedural challenges that can be daunting.”**

In 2008, Congress added a new certification requirement for schools– to certify that, as part of internet safety, schools were educating minors about appropriate on-line behavior, including interacting on social networking websites and chat rooms, as well as cyberbullying awareness and response. Districts continue to be allowed to make local determination of what matters are inappropriate for their students. This determination may be made by the school board or the local administration responsible for the school.

As a part of this process, however, someone within each school district must certify under penalty of perjury that the district is in compliance. That means that each school district is certifying their students are being educated on cyberbullying awareness and response. In practice, however, there is great variance between districts throughout the state as to how cyberbullying awareness and response is taught. This is not to say that such variance equates with noncompliance, but if a district is not moving forward to develop greater infrastructure and instructional presence in this area, the implication is a failure to educate as mandated under the E-Rate relationship.

Student use of technology has grown and, while this poses tremendous potential for educating students, districts are under an obligation when they accept E-Rate dollars to establish sound training practices through all grade levels. Meaningful development or adoption of instructional materials for safe social media use and cyberbullying awareness and response will ensure legitimate compliance as well as fulfill the CIPA’s laudable goals of student education.

Anti-HIB Training Obligations

Even in the event a district does not accept E-Rate dollars, such that certification of student education is not necessary, districts’ general obligation to educate students is reasonably construed to include cyberbullying under the parameters of RCW 28A.300.285, the State’s anti-harassment, intimidation, or bullying (HIB) statute. Under the State definition, HIB includes any intentional electronic act. Districts are required to provide annual training to staff and provision of information to students. Meaningful inventory of how this training and provision of information occurs is recommended for each district.

Bring Your Own Device Trials

Students have broad personal computing device choices to assist with their education: smartphones, tablets, laptops, and netbooks. Some districts have assessed that mobile devices are crucial to student success and have elected to incur significant expense securing such devices. Many districts, however, are increasingly allowing personal devices to be used at school and to connect to district networks. This is commonly referred to as Bring Your Own Device or BYOD. The reasons for this decision usually include cost avoidance, staff support limitations, and a desire to take advantage of the fact that many student possess state of the art devices available for use. Even if cost-reduction is not the primary goal, processing of student data on personal devices is inevitable.

BYOD, however, raises significant data security and privacy concerns. Legal authority is archaic or unhelpful on how to resolve such competing concerns. Students use the same devices they use for school to engage in personal social media, web surfing, email, photos, chat, music, movies, and financial management. Implications of BYOD must be carefully considered

(continued)

and supervision taken into account in developing policies and procedures and appropriate training, including data security, student privacy, IT limitations, and risk management practices. The goal of such an understanding is an approach that strikes a balance between the co-existent interests of personal student privacy and appropriate student supervision even in light of vague legal authority.

FERPA Update Will Bring More Mandates on Technology & Student Information

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of a student's educational record. FERPA's application to current technology and digital communications is ungainly as it has essentially remained the same since its passage in 1974. For instance, such technological milestones as the personal computer, the internet, Wi-Fi, social media, digital photography and video, and Cloud-based services are now in common use in school settings (and often without the knowledge of the central administration). Major possible revisions to FERPA are currently being debated in Congress even as new federal student data privacy legislation also moves forward at the White House's urging.

Members of Congress are generally in agreement that third-party educational technology vendors have gathered, and in public opinion abused, student information for data mining, research, and marketing purposes. Many advocates are concerned that if Congress fails to update FERPA, including clarification of what information can be collected, how that information can be used, and whether or when that information can be shared, student privacy will be at risk. This spurs the need for a FERPA update even further.

A primary focus in updating FERPA is expanding the legal definition of an "educational record" to include the data and metadata generated by software, websites, apps, and online learning platforms. The protection of student information hosted by these third-party educational technology vendors is not currently protected under FERPA. There is also discussion of expanding FERPA to apply to vendors, not just educational agencies, to create greater student privacy and data protections. This is in part a result over concerns over the one-sided contracts or terms of service that districts agree to with third party educational technology vendors that clearly favor the vendors. Another area of concern is standardization of data-security offered by third-party educational technology vendors and data breach notification related to student educational records – something FERPA is resoundingly silent upon in its current state. Many Districts are inconsistent in their technology and data security measures.

Of particular note, there is also some discussion of a graduated set of penalties for FERPA violations and allowance of an individual student cause of action. This likely has its origins in concerns that, despite the growing amount of student data held by districts throughout the country, the current penalty of withholding of federal funds has never been fully used.

A FERPA update will also likely include specific restrictions on what student data technologies can collect and how that data can be used. This will necessitate districts spending time and resources vetting third-party educational technologies to ensure compliance with student privacy.

Take Stock of Your District's Situation

Although updates to FERPA and new regulations may be burdensome, broad support indicates that new legal requirements and related regulations are inevitable. To prepare for such a FERPA remodel and to maintain compliance with such things as E-Rate and HIB training requirements, districts should consider how they utilize educational technology with students, including third-party educational technologies, assess data security and privacy, and confirm educational efforts on social media and cyberbullying. Districts should do this sooner rather than later.

Further, districts should do this in the context of district-specific policies, procedures, guidelines, and practices. WSSDA is working on developing model policies but the scalability of these models is not a one-size-fits-all and the discussion on each district's level will likely be unique. Inevitably, any update to FERPA will likely require greater introspection into student use of technology, student education, and what is appropriate supervision in this new and exciting age of digital communication.

**Charles P.E. Leitch is an attorney and Founding Principal of Patterson Buchanan Fobes & Leitch, Inc., P.S. Mr. Leitch serves as counsel to many Washington school districts. In addition to his litigation practice, Mr. Leitch routinely conducts trainings throughout the Western Hemisphere on supervisory challenges of technology, bullying and cyberbullying response. He has served as a member of the Washington State Attorney General's Youth Internet Safety Taskforce, an Advisory Board member of the Internet Keep Safe Coalition in Washington D.C., and an invited blogger for Yahoo Safely. He is a member of WSSDA's Policy Consulting Cadre.*

> **“Members of Congress are generally in agreement that third-party educational technology vendors have gathered, and in public opinion abused, student information for data mining, research, and marketing purposes.”**