



6 Guidelines for Safe Use of Internet Resources

As teachers and students incorporate Internet tools and new technologies into daily classroom activities more frequently, it is important to be aware of some laws and policies designed to keep kids safe online.



1. Never publish student information on public web sites or blogs.

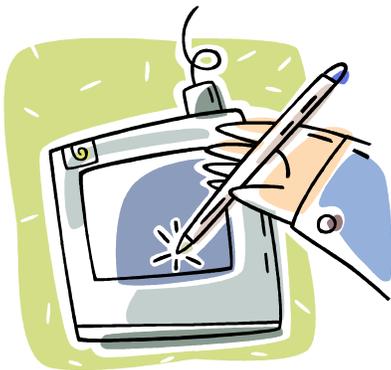
Two federal laws, the [Children's Online Privacy Protection Act \(COPPA\)](#) and the [Children's Internet Protection Act \(CIPA\)](#) require that most students' personal information be kept private at all times. [COPPA](#) states that it is unlawful to collect or display any information that would identify or locate a child (ages 13 and under) without parental consent. [CIPA](#) applies to every computer user in schools and restricts "unauthorized disclosure, use, and dissemination of personal information regarding minors. [under age 18]" Personal information includes, but is not limited to, first and last names, addresses, telephone numbers, likes/dislikes or other personal preferences, or any other information that could be used to identify and/or locate an individual student. Always check with the office staff in your building before publishing or posting student images on the Web, but avoid listing names, etc., with those images. *Never identify a child in anything that is visible online.*

2. Always moderate your blogs, websites, and podcasts, etc.

Once again, [CIPA](#) and [COPPA](#) apply here. If you create a blog, wiki, or personal network for students in class and expect them to contribute to it, or create or subscribe to podcasts that you share with students, make sure you turn the moderation features on. This will require that you approve all comments, edits, and content before they appear publicly to a world-wide audience. If you have a blog, a wiki, a personal network, a web site, or a podcast, you are responsible for all the content and all the comments posted on it. You are also responsible to remove any comments or content that might identify students' personal information (see above). *Always turn moderation features on, and always read through all comments and preview all content before posting.*



3. Always offer a paper/pencil alternative to technology-driven assignments.



Not every child has access to technology resources at home, and sometimes your classroom's or school's computer resources may not be available to students for a variety of reasons. Therefore, you should always have an alternative way to participate in an assignment or class activity that is not dependent on technology. If you want kids to participate in blog posting, allow them to submit ideas on paper as well. If you want kids to do research, encyclopedias and books often contain much more reliable information than Wikipedia, and so on. Also, make sure that the paper/pencil option is worth exactly the same credit as the electronic option. **Never penalize a student for not having a computer or Internet access at home.**

4. Avoid requiring students to sign up for free email accounts.



According to the Children's Internet Protection Act (CIPA), "Schools ... are required to adopt and enforce a policy to monitor online activities of minors" (below age 18). We cannot monitor what we do not provide. Always conduct any electronic communication with students using your District email account. School districts are required by law to keep an archive of all electronic records involving communication with students. This is an effort to protect students, teachers, and school districts from potential liability issues should the student end up in trouble or endangered through use of an email account. Yahoo!Mail, Gmail, Hotmail, and the hundreds of other free online email services do not allow school districts to retain an archive of electronic communications. Requiring students to sign up for these accounts could expose you to enormous legal responsibilities—at your own risk. Should something unpleasant occur, parties involved can be required to produce a record of communications and simply printing paper copies of emails is, in many cases, not sufficient for the legal world (too easy to alter/omit information). Using third-party email services exposes all parties involved to potential legal risk. Therefore, District 205's policy is, and has always been, to neither provide nor encourage student email accounts for classroom use. That's because the District would not be able to support you if something bad were to happen. In short, to avoid exposing yourself and your kids to these risks, *avoid requiring the use of free email accounts with students and **always** use your District email for any student-related communications.*

5. Discuss your online instructional activities with your administrator.



It is always a good idea to make your building administrator aware of your intention to use the technologies mentioned above, and discuss potential ramifications with them before you incorporate these resources in your classroom activities. Even if you follow all the above procedures and take every precaution you can think of, something might happen that you can't foresee. Always provide your administrator the URL (or "web address") of your classroom website, wiki, blog, etc. Some sites allow multiple editors. If so, you might consider allowing your Principal access to your site so they can edit things if an issue comes up and you're unavailable. That's up to you, of course, but remember: they make Principals sit through those School Law classes for a reason, y'know!

6. While it may sometimes be easier to gain forgiveness than permission, it is always easier to gain permission than bail! (*Thanks, Mom & Dad, for that pearl of wisdom during my formative years!*)



The only questions building administrators, District administrators, Technology Department Staff, or even the wandering coordinator can't help you with are the questions you don't ask. No one wants to see you or your students get into unpleasant situations. There are lots of options that we can help you with that may not be out there among the popular culture but will accomplish the same goal as sites like YouTube and so on. *Please let us help you find solutions before they become problems!*

For more information about laws governing student privacy while online, please visit:

Federal Communications Commission on the Children's Internet Protection Act (CIPA): <http://www.fcc.gov/cgb/consumerfacts/cipa.html>

Federal Trade Commission on the Children's Online Privacy Protection Act (COPPA): <http://www.coppa.org/>

OR download their Power Point presentation at <http://www.ftc.gov/bcp/workshops/coppa/COPPARoundtableSlides.ppt>

Questions? Contact Matt Jacobson

District Technology Curriculum & Professional Development Coordinator