Handout for:

Policies 2.0: Rules for the Social Web

Doug Johnson
dougj@doug-johnson.com

Complete set of handouts can be downloaded from:
http://www.doug-johnson.com/dougwri/policies-20-rules-for-the-social-web.html

Session description:
In the fast-changing online world of social networking, where an embarrassing photo can travel the globe in seconds, online predators are the topic of nightly news programs, and young adults travel as avatars to virtual worlds where anything can happen, what policies do schools need to set and how do they set them?

In the spring of 2006, the television news program *Dateline* aired a story about how pedophiles use information gleaned from the social networking site MySpace <www.myspace.com> to locate and abduct children. The story set off a storm of reactions in schools and communities around the nation so strong that even federal legislation was proposed to address this perceived threat to children. Parents learned almost overnight that their children were leading two lives – the one they knew about and one they didn't – online. And if the television news was to be believed, it was a certainty that their children's online activities put them at risk in the physical world.

As a result, schools are still struggling to determine just how to deal with the problems and possibilities of MySpace and other social networking sites.

What is "the social web?"
MySpace is only one incarnation of what is popularly being called Web 2.0, the social web or the read/write web. The simplest explanation of this phenomenon is that the World Wide Web is changing from a "read only" resource to one which user input is not just allowed, but encouraged. The development of online tools that allow content to be entered, uploaded, edited, displayed and made public has made this Web 2.0 possible.

These are some of the more popular manifestations of the social web as of spring 2007. But be warned: new online applications for sharing personal information seem to surface on a weekly, if not daily, basis.

- **MySpace and Facebook** are among the most popular sites where users can easily post information about themselves, create lists of friends, and share comments about interests. According to the Pew Internet & American Life project <www.pewinternet.org/pdfs/PIP_SNS_Data_Memo_Jan_2007.pdf> 55% of all online American youths ages 12-17 use online social networking sites.
- **Blogs** (web logs) started as personal journals, often with highly political overtones. A blog in its most generic sense is a website that is updated on a regular basis, displays the content in reverse chronological order (newest entries first), and allows, even invites, reader response. Technocrati <technorati.com> estimates there are about 55 million blogs as of early 2007.
- **Wikis** are online tools that allow group editing. The most popular wiki is Wikipedia <www.wikipedia.org>, a user-edited encyclopedia that rivals traditional encyclopedias for student use.
- **Social bookmarking** sites such as del.icio.us <del.icio.us> allow users to share their Internet bookmarks and create descriptive "tags" to help organize these resources. **Flickr** <www.flickr.com> does the same for photographs, and **YouTube** <www.youtube.com> allows video tagging and sharing.
- **3-D virtual environments** like Second Life <secondlife.com> and Teen Second Life <teen.secondlife.com> allow users to create avatars, pictorial representations of themselves, and explore these worlds, converse with other avatars, participate in their economies, create habitats, and attend events, some educational.

A comprehensive list of sites for social networking and user created information appears in *The Horizon Report- 2007* published by The Media Consortium and EDUCAUSE <www.nmc.org/pdf/2007_Horizon_Report.pdf>.

How do Web 2.0 safe and ethical use issues differ from those of Web 1.0?
Educators have been concerned about the safe and appropriate use of the Internet for as long as it has been available as a resource in schools. Our district's board-adopted acceptable use policy (AUP) <www.isd77.k12.mn.us/district/isd77policies/524.pdf> reflects the requirements of the Childhood Internet Protection Act (CIPA) of 2001. This law requires schools make efforts to ensure that students cannot access materials that can be classified as "child pornography, obscenity and harmful to minors" and requires that a content filtering system be put in place. When such devices are properly installed and updated, access to content that meets CIPA's definitions can deterred – at least from school networks.

The social web, however, is creating a new set of concerns about safe and ethical behaviors of the Internet by students – ones less easily controlled by mechanical solutions such as filters. These include:

- **Protecting children from predators.** Pedophiles using the information gleaned from sites like FaceBook and MySpace is arguably the area of greatest concern to parents and educators. According to the National Center for Missing and Exploited Children <www.missingkids.com>, "Approximately one in seven youths (10 to 17 years) experience a sexual solicitation or approach while online."

- **Protecting children from each other (cyberbullying).** Nationally recognized Internet safety expert Nancy Willard <www.cyberbully.org> defines cyberbullying as "sending or posting harmful or cruel text or images using the Internet or other digital communication devices," and she documents instances when such activities have resulted severe psychological damage to the victim.

- **Protecting children from themselves (making inappropriate and personal information public)**. Larry Magid and Anne Collier in their book *MySpace Unraveled: What it is and how to use it safely.* (Peachpit, 2006) argue that the greatest likelihood of children and young adults doing harm to themselves on the social web is by posting pictures and messages that portray them in a negative light and that can be viewed by teachers, coaches, relatives, college admission officers, and potential employers. Few students (and adults) understand that material once placed on the Internet and made public has the potential of always being accessible. Projects like The Internet Archive <www.archive.org> store snapshots of the Internet and make them available as historical documents long after websites have changed.

In other words, the danger to kids in Web 2.0 comes not from what they may find online, but from what they themselves put online for others to access.

Our current acceptable use policy (cited above) does include the following language:

> *Users will not use the school district system to post private information about another person, personal contact information about themselves or other persons, or other personally identifiable information, including but not limited to, home addresses, telephone numbers, identification numbers, account numbers, access codes or passwords, labeled photographs or other information that would make the individual's identity easily traceable….*

As educators, we must respond proactively to these real dangers children face in using social networking and read/write web resources. But unfortunately the knee-jerk reaction has been to block *all* social networking resources – blogs, wikis, YouTube, Flickr, and virtual worlds. The well-named, but misguided, Federal 2006 Deleting Online Predators Act (DOPA) proposed last May would have required all schools and libraries receiving E-Rate to filter out all interactive websites since they might lead to students' contact with online predators.

American Library Association president Leslie Berger issued a statement highly critical of the nearly unanimous vote (96%) that passed the bill in the House:

> *This unnecessary and overly broad legislation will hinder students' ability to engage in distance learning and block library computer users from accessing a wide array of essential Internet applications including instant messaging, email, wikis and blogs.*

The attempt to pass similar (and worse) legislation continues. Andy Carvin on his learning.now blog for PBS teachers reports on what he calls "DOPA Jr." <www.pbs.org/teachers/learning.now/2007/01/lifting_the_hood_on_dopa_jr.html>

What is problematic about DOPA and school districts' decisions to block blogs, wikis and chatrooms is that these policies block formats, not contents. In other words, since a student might place personal information on MySpace, all blogs are blocked. This would be like a school banning all magazines because *Penthouse* is published in magazine format. Formats are content-neutral, but many adults seem to be having a difficult time understanding this.

Safety comes from education, not blocking.

Even if social networking sites are effectively blocked in schools, most students will still get access to them. The Pew study cited earlier in this article found:

> *Teens often use the Internet in several locales, especially home and school. This survey shows that teenagers' use of social network sites relates to the place where he or she uses the internet most often. Teens who go online most often from home are more likely to report using social network sites than are teens who go online most often from school (42%). Home users are more likely to have profiles posted online (59% compared with 38%) and are more likely to visit social networks once a day or more frequently than are those who go online mostly from school.*

Proxies and mobile networking devices also help the ambitious student avoid district filtering efforts. Do you know about SchoolBoredom.com <www.schoolboredom.com/>? Trust me, your kids do. Highly portable, personal networking devices that use cell phone signals to access the Internet are gaining in popularity among students – who, of course, bring them to school.

To think simple Internet filters will eliminate or even minimize the real risks associated with social networking, is a dangerous misconception. **It will take educating students about the appropriate use of the Web 2.0 to genuinely protect them.**

Responsible adults are using online curricula from organizations like iLearn <ilearn.isafe.org/>. (See sidebar for a list of resources for parents and teachers.) One site, NetSmartz, has created eye-opening videos such as "Tracking Theresa" and "Julie's Journey" <www.netsmartz.org/resources/reallife.htm>. Teachers find these ready-made curricula simple to integrate into their classrooms when teaching safety units.

Our school district, like others, has been actively working to educate communities and parents on issues surrounding Internet safety. We have developed a resource list of websites for parents about safe Internet use <www.isd77.k12.mn.us/parents>, have worked with our parent-teacher organizations and community education department to arrange programs about the topic, and have sent home reminders about good computer use in building newsletters home.

The need for the social web in schools – and children's lives

Pioneering educators are finding exciting ways to make good use of Web 2.0 resources. Schools and libraries are replacing their newsletters with blogs that can be rapidly updated and allow readers to respond. Teachers are using wikis to facilitate peer-reviewed and collaborative writing projects – including student created textbooks. Social book marking sites are proving to be an efficient means of creating bibliographies and reading lists. Creative teachers are asking students to create Facebook-like profiles for literary characters. (Who *would* be on Juliet Capulet's friends or music favorites list?) Virtual literary worlds are allowing students to walk through Orwell's world of *1984* and Richard Wright's *Native Son* Chicago setting.

But the issues are larger than these resources simply being used to facilitate traditional learning experiences. Henry Jenkins Director of the Comparative Media Studies Program at the MIT and author of the McArthur report, *Confronting the Challenges of Participatory Culture* <www.digitallearning.macfound.org> writes: "We are using participation as a term that cuts across educational practices, creative processes, community life, and democratic citizenship. Our goals should be to encourage youth to develop the skills, knowledge, ethical frameworks, and self-confidence needed to be full participants in contemporary culture," he asserts, and adds, "What a person can accomplish with an outdated machine in a public library with mandatory filtering software and no opportunity for storage or transmission pales in comparison to what person can accomplish with a home computer with unfettered Internet access, high bandwidth, and continuous connectivity… The school system's inability to close this participation gap has negative consequences for everyone involved."

Obviously, districts must create a balance between opportunity for student engagement and new teaching methods and the need to protect children. But it is not a simple determination to make.

How are good decisions made about filtering and policy?
Look at the language of CIPA – "obscene, child pornographic and harmful to minors." These terms are open to a broad range of interpretations. Our own district's board set AUP includes phrases like:

- The school district system has a limited educational purpose, which includes use of the system for classroom activities, professional or career development, and limited high-quality, self-discovery activities.
- Users will not use the school district system to access, review, upload, download, store, print, post, or distribute materials that use language or images that are inappropriate to the educational setting
- An individual investigation or search will be conducted if school authorities have a reasonable suspicion that the search will uncover a violation of law or school district policy.

"High-quality," "inapropriate," "reasonable." Lovely, but ambiguous terms. Again, all open to interpretation.

Which leads to questions like this that I hear regularly from teachers and students – "Is there any definitive answer to what should or should not be filtered to meet CIPA requirements? Our technology director has been checking more little boxes on our filter." Or, "Our district has blocked access to all blogs. How can we get this policy changed?"

Who in a school *should* ultimately decide what is blocked and what is accessible to students and staff?

Ultimately, school boards rule on specific instances of resource selection. But in our district, these daily procedural, rather than policy decisions, are made by our district Technology Advisory Committee, the same folks who make lots of technology planning and budget decisions. This committee is comprised primarily of educators - teachers, media specialists, and administrators - but also includes parents, students, businesspersons, college faculty members, and public librarians. And of course the committee includes our technical staff for their important input on security, compatibility and implementation issues. And we DO listen to everyone. Most of our building technology committees work in the same way. (You can find some tips on forming and running an advisory group at <www.doug-johnson.com/dougwri/ advice.html>.)

Sara Kelly Johns 3/8/07 12:56 PM
Comment: For emphasis, make it a proper noun

This has worked well for us. On the difficult filtering issue for example, the committee decided that as a result of CIPA, we would install a filter, but it would be set at its *least* restrictive setting. Any teacher or librarian can have a site unblocked by simply requesting it – no questions asked. Adults are required to continue to monitor student access to the Internet as if no filter were present. The technicians know that it is the responsibility of the teaching staff to see that students do not access inappropriate materials, not theirs. This is a good policy decision that could not have been reached without a variety of voices heard during its making. And has held up well even as Web 2.0 resources have become available.

It is also a decision that I believe honors the spirit of intellectual freedom – that a resource is innocent until proven guilty. If anyone requests that a site or resource is blocked, the same due process accorded to print or audio visual materials is followed unless it is immediately apparent that the resource violates the "obscene, child pornography or harmful to minors" dictate of CIPA. Without a formal process for the blocking of Internet-based materials, censorship becomes a real possibility. When a teacher complains to me when I refuse to block a game site, I explain that if I blocked every individual request, I would have to honor the request of the next parent who asks that a political or religious site is blocked. And I add that a formal reconsideration request can be made using the same form used to remove print instructional materials from the school.

Vicki Davis on her Cool Cat Blog <coolcatteacher.blogspot.com/2007/02/including-classmate-with-leukemia.html> reflects:

...it is not the tools that are inherently good or evil but rather the use of the tools.
A hammer can kill someone but it can also build a house.
A nail can be driven through a hand but it can also hold the roof over your head.
A fist can hit but a fist can also be clasped in your hand in love.

We do not outlaw hammers, nails, or fists -- we teach people to use them properly.

So should we do with blogs, wikis, podcasts, Skype, and any other tool that becomes available for use in the human experience!

Well said.

Links Mentioned (checked June 2008)

- MySpace <www.myspace.com>
- Pew Internet & American Life Project, Jan 2007 <www.pewinternet.org/pdfs/PIP_SNS_Data_Memo_Jan_2007.pdf>
- Technocrati <technorati.com>
- Wikipedia <www.wikipedia.org
- del.icio.us <del.icio.us>
- Flickr <www.flickr.com>
- YouTube <www.youtube.com>
- Second Life <secondlife.com>
- Teen Second Life <teen.secondlife.com>
- The Horizon Report- 2008 < <www.nmc.org/pdf/2008-Horizon-Report.pdf >.
- ISD77 Acceptable Use Policy <www.isd77.org>
- Larry Magid and Anne Collier (book) *MySpace Unraveled: What it is and how to use it safely.* (Peachpit, 2006
- The Internet Archive <www.archive.org>
- Andy Carvin, learning.now blog "DOPA Jr." <www.pbs.org/teachers/learning.now/2007/01/lifting_the_hood_on_dopa_jr.html>
- "Tracking Theresa" and "Julie's Journey" <www.netsmartz.org/resources/reallife.htm>
- Gargoyles Loose in the Library blog http://www.uni.uiuc.edu/library/blog/index.html
- Hennepin County Library in MySpace <www.myspace.com/hennepincountylibrary>
- Wikibooks <en.wikibooks.org/wiki/Main_Page>
- Virtual literary worlds <brn227.brown.wmich.edu/literaryworlds/>
- Confronting the Challenges of Participatory Culture <www.digitallearning.macfound.org>
- Tips on forming and running an advisory group at <dougjohnson.squarespace.com/dougwri/advisory-advice.html>
- Student guide to cyberbulling <doug-johnson.squarespace.com/blue-skunk-blog/2008/2/4/student-guide-to-cyberbullying.html>
- Vicki Davis, Cool Cat Blog <coolcatteacher.blogspot.com/2007/02/including-classmate-with-leukemia.html>
- Predators & cyberbullies: Reality check
- <www.blogsafety.com/thread.jspa?threadID=1100000263&tstart=0>

Sidebar: Recommended websites about Internet safety for parents

- Center for Safe and Responsible Internet Use <csriu.org>
- Children's Partnership <www.childrenspartnership.org>
- ConnectSafely <www.connectsafely.org/>
- CyberBullying information <www.cyberbully.org>
- CyberSmart <cybersmart.org>
- Family Guide Book <www.familyguidebook.com>
- Get Net Wise <www.getnetwise.org>
- iKeepSafe.org <ikeepsafe.org/PRC/>
- McGruff Online Safety for Kids <www.mcgruff.org/advice/online_safety.php>
- MediaWise <www.mediafamily.org/resources.shtml>
- National Center for Missing and Exploited Children <www.ncmec.org>
- NetLingo: Top 20 Internet Acroynms Every Parent Needs to Know < www.netlingo.com/top20teens.cfm>
- NetSmartz <www.netsmartz.org>
- Play It Cyber Safe <www.playitcybersafe.com>
- SafeKids.com <www.safekids.com>
- SafeTeens.com <www.safeteens.com>
- Wired Safety Website <www.wiredsafety.org/parent.html>