Web 2.0--Pros or Cons

With the use of Web 2.0 tools, there comes the challenge of using them effectively and properly while dissipating the threats that go along with their use. There are many advantages to using the tools inside schools and corporations however, there are also threats to the networks that cannot be ignored. As with any web-based tool, there are security risks involved with usage. Not only are there threats to the network, but there are also risks to the user. In today's society, administrators must take precautions to protect the network and the user.

Inside classrooms and corporations Web 2.0 tools have some unique advantages that have never been present before. These tools allow users to "create strong communities of practice, essential aids to good teaching and learning (Groff & Haas, 2008)." Students, teachers, and employees are able to experience real life applications to learn and connect to the world. Students are learning in ways that will help them to develop as positive contributors to society. The technology is engaging students that may have otherwise disassociated themselves with schoolwork.

Technology is what students know; it is how they grow up, how they live their lives. Students explore social networks at home, they play video games, and they are generally more familiar with the Internet then their teachers and parents. One thing that students do not always recognize is the risk that goes along with using these tools. According to a survey done in 2006, principals and administrators said that their greatest concerns for students online were pornography, adult predators, and useless or irrelevant results when using search engines. Seventy-six percent of those surveyed had concerns over unauthorized redirection to commercial or pay sites when conducting research (Solomon & Schrum, 2007, p. 140).

Among these valid concerns, network administrators must also protect the integrity of the network. By allowing web 2.0 tools through the network, there becomes a vulnerability for misuse and hacking. According to Anthony Plewes, "most security threats that affect web 2.0 are not new. They stem from issues with browser design and web architecture that did not anticipate how the web would be used in the future (Plewes, 2007)." Hackers are finding more and more ways to get into networks, infect them, and ultimately bring them down. Different websites pose different threats for networks. It is the job of the network administrator to prevent these threats from getting through and to keep the information on the network safe and secure.

To prevent the risks from getting through a network, filters are often put into place. Despite these filters, there are still some problems with sites getting through or results from searches being inappropriate. In addition to filters, districts and corporations have implemented acceptable use policies (AUP). In the past, these policies have outlined the guidelines, procedures, and responsibilities for using technology. As these new technologies emerge, districts and corporations must revisit their acceptable use policies to include the new online tools. The policy needs to be clear for students and staff to know what is permitted and what is not (Solomon & Schrum, 2007, p. 144).

In order to use the technology effectively, the teacher and employer must first be able to use it properly. By offering professional development and proper training, staff can become proficient in the tools and then can distribute that knowledge to others. The acceptable use policy protects the district or corporation against the misuse of technology. If this misuse does occur, the organization has a means to deal with the problem legally. Even with the use of AUPs, there are still threats and the network administrator must decide which sites and tools are worth the risk and how to prevent the threats.

There are so many different aspects of web 2.0 that need to be considered when determining what is and what is not appropriate for different settings. There are some people who believe social networks such as My Space and Facebook have a place in schools and businesses. It is my opinion that these specific social networks are not appropriate for the environments in question and should therefore be blocked for the network. It is up to the network administrator to pick and choose what is able to get through. These administrators should start with applications and tools that staff are knowledgeable about and that can be monitored within the network. If a staff member has a valid reason and justification of use, it would be beneficial to have them "pilot" it's use. After this, any other staff members who would like to use it would be required to undergo training to assure proper use of the tool. As the years progress, the hope would be to become advanced users of certain tools and continue to introduce other tools for use.

In any setting it would be important to research the security of sites and how their networks will interact with the school's or corporation's networks. The use of web 2.0 tools is still new to the world and the first thought would be to not allow them. Doing this, in my opinion, would be a disservice to those the network administrator serves. These tools are the future of the Internet and will not lesson in their importance to advancement.

Web 2.0 tools in general can provide students and employees an opportunity to experiment with thing in the “real world” that would otherwise be out of their reach. Depending on what skills you are trying to impart or learn, the Internet offers a multitude of applications and tools that will enhance the learning environment. One example of this is Ayiti, a digital game that gives the user authority over a family to help them make decisions about their work, education, community building, personal purchases, and health care in order to improve their lives. Students are expected to evaluate situations and make the decisions based on what would be best for the character. There are also many other games that help students simulate situations where they could have just read a textbook before (Groff & Haas, 2008).

Educators should be taking advantage of the tools that have been created for specific use in schools. Some examples of education related tools include www.pbwiki.com, www.edublogs.org, and www.classblogmeister.com. These sites all allow for administrative security and provide an environment for students to create their own learning space and connect to others. The main focus of web 2.0 tools in classrooms should be to form learning communities, not social ones. In using these, students are also learning proper behaviors and how to keep themselves safe when on the Internet (Solomon & Schrum, 2007, p. 156). The aforementioned websites provide a collaborative environment where the person named as administrator on an account can control what is posted and what goes on. These are just three of many sites that can be used to enhance learning.

Many districts and corporations setup a firewall to protect their network. This firewall filters what information comes into the network and can block out potential information that could be harmful to the network. This is put into play to prevent hacking, viruses, spam, and other dangers. This filtering system can catch beneficial information and prevent it from entering the network; this is one of the many problems that administrators face. Technology planning committees are working on this among many challenges to keep the network and it's users safe (Solomon & Schrum, 2007, p. 152).

Another solution to the threats of web 2.0 tools is to place the tools directly on the intranet, behind the firewalls of the district. This solution does limit the collaboration that can occur within the classroom, but it still allows the students and staff to collaborate with each other and across classrooms (Solomon & Schrum, 2007, p. 156). Keeping the threat contained in a manageable environment gives the user the opportunity to utilize the technology to impart learning.

As the network administrator, I would need to keep the network safe, but I must also consider what the tools will be used for. There will always be people who are more capable of using the technology and there will always be people who will test the limits of use. The AUP, if written well, will be the guiding point to fall back on to protect the integrity of the network. Those who sign the AUP know the expectations of use and should understand the consequences if they choose to violate it.

In the end, every district or corporation must make a decision as to what is useful and what is not. The skills used may or may not be more relevant then the threat posed to the network. Each site should be evaluated individually and a conclusion should be made based on the results. An overall ban on all web 2.0 sites does not seem to be the logical answer. Rather, allow those sites that will benefit the organization while proving to be as small of a threat as possible. In most situations, I think that students and employees will find more relevance in their work this way.

References:

Solomon, G., & Schrum, L. (2007). *Web 2.0 new tools, new schools*. Washington DC: International Society for Technology in Education.

Plewes, A (2007, November 26). Web 2.0 threat looms- Research-Breaking Business and Technology News at silicon.com. Retrieved November 22, 2008, from www.silicon.com Web site: http://www.silicon.com/research/specialreports/digitaldefences/0,3800014341,39169267,00.htm?r=6

Groff, J, & Haas, J (2008, September/October).Web 2.0 Today's Technologies, Tomorrow's Learning. *Learning & Leading*, *36*, 12-15.