PARTICIPATORY Learning
LEADERSHIP & POLICY
A COSN LEADERSHIP INITIATIVE

Acceptable Use Policies in a Web 2.0 & Mobile Era

A Guide for School Districts

Information and communications technologies (ICT) policies in schools have two dimensions. One is to ensure that students are protected from pernicious materials on the Internet. The other is to enable student access to the extensive resources on the Internet for learning and teaching. While these two dimensions are not intrinsically in conflict, in actuality, such can become the case.

There is a wide range of restrictiveness with regard to Internet access in school districts across the U.S. A critical concern is: How can we best assure that students will not be affected by pornography, hate sites, sexual or physical harassment, and other pernicious sites and situations that exist on the Internet? Some districts believe that the best way to do this is to rely on blocking and filtering to eliminate access to harmful sites. Other districts take a different policy stand. While they also use blocking and filtering that federal law requires, their policy is based on the premise that children need to learn how to be responsible users and that such cannot occur if the young person has no real choice. School personnel who take this stand contend that students need to acquire the skills and dispositions of responsible Internet usage and to be held accountable for their behavior. Moreover, those holding this position contend that restrictive school networks may provide more of an appearance of protection than reality since they can be bypassed by students. Schools with less restrictive environments often distinguish between the restrictiveness appropriate for older and younger students since young children may stumble across sites they ought not visit.

Web 2.0 applications and mobile Internet devices have added new issues to the safety/access situation for schools. The purpose of this guide is to assist school districts in developing, rethinking, or revising Internet policies as a consequence of the emergence of Web 2.0, and the growing pervasiveness of smart phone use. The CoSN Policy Guide addresses these questions:

1. **How does policy differ from procedure and does the difference matter?**
2. **What are the two major approaches used to develop district AUP policies?**
3. **Is the district's AUP a part of or the totality of the district's technology policy?**
4. **What are the key federal laws affecting Internet access, safety, and social networking in schools?**
5. **How do state laws or district policies affect school districts' Internet policies pertaining to filtering, AUPs, cyberbullying, and cell phone use?**
6. **Does the increasing prevalence of Web 2.0 and student-owned mobile devices necessitate updating district ICT policies?**
7. **Where can I find samples of various exemplary AUPs?**
8. **What are some timely, relevant, and useful resources pertaining to the use of Web 2.0 technologies in schools?**

1. How does policy differ from procedure and does the difference matter?

Policies are principles or rules that are intended to shape decisions and actions. They provide the framework for the functioning of the organization. *Procedures* are the ways that organizations implement policies. Policies answer the "what" and "why" questions. Procedures answer the "how," "who," and "when" questions. Policies are expressed in broad terms; procedures in more specific behavioral or operational terms. Since procedures need to be more flexible to adapt to changing conditions in the organization, it is useful to differentiate policies from procedures so that procedural modifications can be made in a timely manner—often without board action.

2. What are the two major approaches used to develop district AUP policies?

School districts have approached policy development pertaining to ICT in one of two ways: 1.With a school official such as the chief technology officer, a cabinet member, or legal counsel working alone, or with one or two others; 2.With involvement of a committee comprised of stakeholders including parents, teachers, administrators, community members and (though more rarely) students. While the former approach is easier and more efficient, a more inclusive process will result in better policy and more "buy-in" from those who are affected by the policy. Critical to the success of AUP policies is the sense of ownership of the policies by their prime target: students. Ownership requires that students understand the policies, the reason why they are put in place, and accept them. Student involvement in policy formation can help to generate student "buy in." The Littleton Public School District and the Broward County Public School District are examples of two districts that have established technology committees with broad representation from key stakeholders. Some districts, such as the Portsmouth School Department, have altered the perspective on "acceptable" use policies by framing them as "responsible" use policies. The need for broad-level understanding and support of the total school community for AUP policies is particularly acute with regard to social networking and handheld Internet devices due to widespread student use and is fraught with more complex issues pertaining to control than when dealing simply with strictly district-owned equipment.

3. Is the district's AUP a part of or the totality of the district's technology policy?

AUP policies are focused on preventing harm to students or abuse of the district's computer network. In many instances, the perspective of the AUP seems to imply that ICT contains more risks than benefits. Federal law (CIPA, described in section 4 below), and in some instances state law or state department of education policy (as described in section 5 below), requires

districts to establish rules for behavior. It is less common for school districts to frame their AUP within a context of the benefits or necessity for the use of ICT in teaching and learning. Bellingham Public School's AUP is an example of a district policy that provides a policy endorsement and rationale for the use of ICT as a critical component of the teaching/learning process.

4. What are the key federal laws affecting Internet access, safety and, social networking in schools?

The Children's Internet Protection Act (CIPA) is the key federal law affecting ICT use in schools. A brief document explains the key provisions of CIPA. The law requires any school district that receives E-Rate funding to filter or block visual depictions that are obscene, that contain child pornography, or material harmful to minors. Schools are required to enforce the operation of such technology protection measures (i.e., keep the filter operating) during any use of such computers by minors. The law also requires districts to have in place a policy of Internet safety that includes the use of a filter or blocking procedure for district computers used by minors. CIPA became law in 2000—before the emergence of Web 2.0—and thus does not stipulate any specific requirements for school districts using social networking or other Web 2.0 applications. Title II of the Broadband Data Improvement Act, which became Public Law 110-385 on October 10, 2008, is titled, "Protecting Children in the 21st Century." Section 215 is most relevant to schools and requires them, as part of their Internet safety policy, to educate minors about appropriate online behavior. This includes how to interact with others on social networking websites and in chat rooms as well as cyberbullying awareness and response.

The State of Washington Department of Public Instruction Website contains background documents for developing an AUP, a template for an AUP, and a compilation of current research pertaining to child safety issues.

5. How do state laws or district policies affect school districts' Internet policies pertaining to filtering, AUPs, cyberbullying, and cell phone use?

A number of states have enacted legislation pertaining to Internet use in schools. The legislation falls into two categories. One type of legislation is generally redundant with federal law and requires school districts to filter or block harmful materials. The most common explanation for the redundancy is the threat of the removal of state funds. The other type of legislation calls for protecting children from cyberbullying. See Table (1) State Laws Pertaining to Filtering and Cyberbullying.

In the wake of several instances of serious harm to children resulting from the pernicious use of social networking, a number of state boards of education have also enacted state requirements for school districts pertaining to bullying, hazing, and harassment. State legislation is a fluid process and one should check with the appropriate state government to get the most up-to-date information on laws.

This is particularly important in upcoming state legislative sessions where many new governors and state legislative bodies have changed party control.]

Many school districts *allow* social networking that has been devised for schools and includes protections in the form of restricted access, filters, or monitors—but *block* the most widespread social networking applications such as Facebook, Myspace, and Twitter. However, a growing number of districts allow them for classroom use and for communication between school personnel with parents and others in the community. *eSchool News* story entitled *"Schools still conflicted over Web 2.0 tools*" summarized CoSN's Compendium article *Web 2.0 as a Force for School Transformation: A Tale of Six Districts* that provided profiles of six school districts that are reducing restrictions of Web 2.0 applications. Districts that are less restrictive with regard to filtering and blocking contend that cell phone use in schools continues to be a contentious issue, but there is a trend to reduce and relax the restrictions. Policies on cell phone usage vary from districts that forbid students from bringing them into the school building (such as the Student/Parent Handbook in the New Haven's Connecticut schools), to schools that provide for limited use, to schools which are making use of them for instructional purposes (i.e. Carlisle Area School District, Cumberland Valley High School). The increasing prevalence of cell phones is prompting a growing number of school districts to revise their policy on cell phones. Prominent education leaders including the executive director of the American Association of School Administrators are calling for less restrictive policies regarding smart phones. An article in *Education Week* reports on schools opening doors to students' mobile devices.

6. Does the increasing prevalence of Web 2.0 and student-owned mobile devices necessitate updating district ICT policies?

School districts take differing positions on updating their AUP. Some districts update if and when a crisis, issue, or situation indicates a need for policy change. Others schedule periodic updating. There are two reasons why regular district updating may be useful. The first is that information technology is quite dynamic. Information and communications technologies continue to develop and evolve—and the perspectives on teaching and learning that pertain to the use of ICT also change.

The second reason for periodic updating of policies is to perpetuate ownership of them by those whose activities are affected by them. Effective policies do not live on paper; they live in the consciousness of those whose lives the policies affect.

The increasing use of Web 2.0 applications in the home and the increasing prevalence of smart phone ownership by school age youth are key factors in causing many districts to have to review their AUP and to include provisions pertaining to Web 2.0 and smart phones. Events of cyberbullying leading to tragic consequences that have received widespread publicity have also prompted many school districts to develop a policy pertaining to cyberbullying and, though less frequently, sexting. Also, as indicated above, the law requires school districts to "to educate minors about appropriate online behavior, including online interaction with other individuals in social networking web sites and in chat rooms and cyber-bullying awareness and response." Districts may choose to stipulate their adherence to this law in a policy statement, but such is not required by the law.

Given the increasing extent of use of cell phones and other mobile technologies by students, the need for formal policy pertaining to personally-owned mobile devices is clear. An article in the *EdTech Newsletter* provides information on AUPs in a Web 2.0 world. A number of school districts throughout the U.S. are revising cell phone policies, and schools that previously banned cell phone from school property are now permitting their use before classes begin, during lunch, and after classes end. The rationale for this is to enable children and parents to be able to be in (at least limited) contact. A growing number of school districts, such as the Dysert School District in Arizona, are permitting their use in teaching and learning in the classroom.

There are two positions on specifying Web 2.0 applications in district policy particularly for those districts that are favorable to the use of Web 2.0. School districts that ban social networking or other Web 2.0 applications such as blogs, YouTube, etc. typically write the proscription into their AUP policy. Some districts that are less restrictive believe that it is important to specify the use of Web 2.0 as acceptable to minimize misunderstanding about the legitimacy of the use in the district. Also, less restrictive districts may see the need to specify the parameters for Web 2.0 use and to define what uses are inappropriate, unethical, or illegal. Other districts believe that it is better to deal with acceptable and unacceptable use of Web 2.0 in a more generic manner, as ICT applications in use in the district, without tying such to specific types of applications.

7. Where can I find samples of various exemplary AUPs?

Barrington Public School District, IL. Mentions the different types of learning tools and how they are necessary for learning.

Bellingham Public Schools, WA. Deals with unacceptable behavior in a generic manner rather than singling out Web 2.0 applications. Provides a one-sentence statement that requires staff to provide students with "guidance and instruction" on the appropriate use of information resources. AUP policy is an example of a district policy that provides a policy endorsement and rationale for the use of ICT as a critical component of the teaching/learning process.

Broward County Public School District, FL. This school district established a technology committee to include key stakeholders to develop their AUPs.

Duxbury Public Schools, MA. Contains language specific to Web 2.0.

Dysert School District, AZ. AUP includes the use of microblogging, mobile devices, social networking and staff websites.

Edina Public Schools, MN. Detailed, and includes a statement pertaining to harassment and personal attacks.

Fairfax County Schools, VA. A policy document pertaining to the use of privately-owned computer devices on the District network.

New Canaan School District, CT. Mentions how the Director of Technology and r epresentatives can modify or disable any technology protection measures.

Littleton Public Schools, CO. This school district established a technology committee to include key stakeholders to develop their AUPs.

Springfield Public Schools, MO. A typical AUP, it specifies unacceptable behavior as well as sanctions for such.

Warwick School District, PA. Contains the Warwick School District policy on cyber-bullying and related matters.

8. What are other resources for use in responding to the policy issues pertaining to Web 2.0 technologies in schools?

Varying Approaches to Internet Safety. A discussion with senior officials from Ministries of Education, national information and communication (ICT) policy bodies, or national school networking organizations from Denmark, Sweden, The Netherlands, UK, the USA and Australia on Internet Safety.

Web 2.0 as a Force for School Transformation: A Tale of Six Districts, CoSN Compendium. Contains brief profiles of six districts approach to dealing with Internet safety and access. Read Web 2.0 as a Force for School Transformation (Executive Summary) (Full Article- CoSN members' resource, also available for purchase).

Maine International Center for Digital Learning. Provides a comprehensive document for use in developing an AUP.

Social Media Guidelines for Schools. A wiki for collaboration on developing social media guidelines for schools.

Cyber Security for the Digital District. This website provides information and tools to help school districts protect their networks, and to assist them in using technology for teaching and learning.

Empowering Parents and Protecting Children in an Evolving Media Landscape. From the Berkman Center for Internet and Society at Harvard University, this report provides a detailed review of research and policy pertaining to Internet safety for children.

James Bosco
Principal Investigator
Participatory Learning in Schools: Leadership & Policy
Consortium for School Networking

This is made possible with support from the John D. and Catherine T. MacArthur Foundation under the Digital Media and Learning initiative. Additional support from Adobe, eChalk, Gartner, GlobalScholar, Learning.com, Pearson, SAS, and Smart Technologies.

Consortium for School Networking
1025 Vermont Avenue, NW, Suite 1010, Washington, DC 20005
866.267.8747
www.cosn.org
www.cosn.org/membership
info@cosn.org

State Laws Pertaining to Filtering and Cyber-bullying

State	Internet Filtering Laws in Schools	Cyber-bullying
Arizona	Requires public libraries to install software or develop policies to prevent minors from gaining access on the Internet to materials harmful to minors. Requires public schools to install computer software that would prevent minors from gaining access to materials harmful to minors. Citation: Ariz. Rev. Stat. Ann. § 34-501 to -502	
Arkansas	Requires school districts to develop a policy and to adopt a system to prevent computer users from accessing materials harmful to minors. Requires public libraries to adopt a policy to prevent minors from gaining access to materials harmful to them. Citation: Ark. Code § 6-21-107 (pg 865), § 13-2-103 (pg 4).	Includes electronic acts that create a "clear and present danger" of physical harm, "substantial interference" with education, a "hostile educational environment" or "substantial disruption" of the school. The prohibited "electronic acts" include off-campus communication that is "directed specifically at students or school personnel and maliciously intended for the purpose of disrupting school, and has a high likelihood of succeeding in that purpose." Citation: H.B. 1072, 2007: Arkansas Code, §6-18-514(a)
California		Prohibits bullying through electronic means that is directed specifically toward a student or school personnel. Students may only be punished for acts that are "related to school activity or school attendance occurring within a school under the jurisdiction of the superintendent of the school district or principal or occurring within any other school district." Does not explicitly provide for punishment of off-campus electronic bullying. Citation: A.B. 86, 2008: California Education Code Annotated §32261
Colorado	Requires public schools to adopt and enforce reasonable policies of Internet safety that will protect children from obtaining harmful material. Provides grants to publicly supported libraries, including school libraries, that equip public access computers with filtering software and that have policies to restrict minors from accessing obscene or illegal information. Requires public libraries to adopt a policy of Internet safety for minors that include the operation of a technology protection measure for computers with Internet access. Citation: Colo. Rev. Stat. § 22-87-101 to 107	
Delaware		Prohibits bullying through electronic means that a reasonable person should know will place a person in fear of harm to emotional or physical well-being, create a hostile educational environment, interfere with a safe school environment, or incite bullying in third parties. Requires that bullying have a "sufficient school nexus." Citation: H.B. 7, 2007: 14 Delaware Code §41120
Florida		Prohibits bullying during educational programs and activities, during school-related or -sponsored activities, on school buses, and through the use of computers or software accessed on a computer, computer system or computer network of an educational institution. Citation: H.B. 669, 2008: Florida Statutes §1006.147

State Laws Pertaining to Filtering and Cyber-bullying

State	Internet Filtering Laws in Schools	Cyber-bullying
Georgia	Requires public schools and public libraries to adopt and enforce reasonable policies of Internet safety that will protect children from access to harmful material. Prohibits a public school or library from receiving state funds unless it implements and enforces the acceptable-use policy. Citation: Ga. Code § 20-2-324	
Idaho		Prohibits bullying that a reasonable person should know will have the effect of harming a student, damaging a student's property, placing a student in reasonable fear of harm, or placing a student in reasonable fear of damage to his or her property, and that creates an intimidating educational environment for a student. Provides that bullying may occur through the use of computers or telephones. Does not mention location. Citation: H.B. 750, 2006: Idaho Code Annotated §280.28
Iowa		Prohibits bullying through electronic acts that is based on any actual or perceived characteristic of a student and that creates an objectively hostile school environment by placing a student in reasonable fear of harm, causing a substantially detrimental effect on a student's health, substantially interfering with a student's academic performance, or substantially interfering with a student's ability to benefit from and participate in school activities. Does not mention location. Citation: S.F. 61, 2007: Iowa Code §280.28
Kansas		Prohibits "cyberbullying," intentional acts through electronic means that create an intimidating educational environment for a student or school personnel and that a reasonable person should know will have the effect of harming a student or staff member, damaging student or staff property, or placing a student or staff member in reasonable fear of harm or damage to property. Provides that school boards will prohibit cyberbullying on or while utilizing school property, in a school vehicle, or at a school-sponsored event. Citation: H.B. 2758, 2008: Kansas Statutes Annotated §72-8256
Kentucky	Requires the Department of Education to develop regulations to prevent sexually explicit material from being transmitted via education technology systems. Citation: Ky. Rev. Stat. § 156.675	
Louisiana	Requires schools to adopt policies regarding students' and school employees' access to certain Internet and online sites. Citation: La. Rev. Stat. Ann. § 17:100.7	

State Laws Pertaining to Filtering and Cyber-bullying

State	Internet Filtering Laws in Schools	Cyber-bullying
Maryland		Prohibits bullying, which is intentional conduct or intentional electronic communication that creates a hostile educational environment and is motivated by an actual or perceived personal characteristic or is threatening, and occurs on school property or "substantially disrupts the orderly operation of a school." Citation: H.B. 199, 2008: Maryland Education Code §7-424, 7-424.1
Minnesota		Provides that each school board shall adopt a written policy prohibiting bullying through electronic means. Citation: S.B. 646, 2007: Minnesota Statutes §121A.0695
Missouri	Requires public school and public libraries with public access computers to either (a) equip the computer with software or a service to restrict minors' access to material that is pornographic for minors, or (b) develop a policy that establishes measures to restrict minors from gaining access to such material. Citation: Mo. Rev. Stat. § 182.827	Prohibits using electronic or any other means of communication to knowingly "frighten, intimidate, or cause emotional distress to another person," making "repeated unwanted communication to another person" or using unwanted or offensive communication that "puts [a] person in reasonable apprehension of offensive physical contact or harm." Citation: S.B. 818, 2008: Missouri Revised Statutes, §565.090, §565.225
Nebraska		Prohibits bullying, including through electronic means that occurs on school grounds, in a school vehicle, or at school-sponsored events. Definition of bullying is not fully developed. Citation: L.D. 205, 2008: R.R.S. Nebraska 121A.069579-2,137
New Hampshire	Requires school boards to adopt a policy regarding Internet access for school computers, and establishes liability for violation of the policy. Citation: N.H. Rev. Stat. Ann. § 194:3-d	
New Jersey		Prohibits bullying through electronic means that is motivated by an actual or perceived characteristic and that a reasonable person should know will have the effect of harming a student or a student's property or placing a student in reasonable fear of harm to self or property, or has the effect of insulting a student or group of students in such a way to cause substantial disruption of school, and takes place on school property, on a school bus, or at a school-sponsored function. Citation: S.B. 993, 2007: New Jersey Statutes §18A:37-14

State Laws Pertaining to Filtering and Cyber-bullying

State	Internet Filtering Laws in Schools	Cyber-bullying
Oklahoma	Directs all state agencies and educational institutions to keep computer systems free from obscene materials. Citation: 1996 H.C.R. 1097 (uncodified)	Prohibits harassment, intimidation and bullying by any gesture, written or verbal expression, electronic communication, or physical act that a reasonable person should know will harm another student or damage another student's property, place another student in reasonable fear of harm to the student's person or damage to the student's property, or insult or demean any student or group of students in such a way as to disrupt or interfere with the school's educational mission or the education of any student. Law pertains to schools or school-sponsored activities. Requires each district board of education to adopt a policy on bullying. Citation: S.B.1941, 2008: 70 Oklahoma Statutes §24-100.3
Oregon		Provides that each school district shall create a policy prohibiting cyberbullying, which is the use of any electronic communication device to harass, intimidate or bully. Citation: H.B. 2673, 2007: Oregon Revised Statutes §339.351, §339.356
Pennsylvania		Requires school systems to develop policies prohibiting bullying, including through electronic means. "A school entity shall not be prohibited from defining bullying in such a way as to encompass acts that occur outside a school setting if those acts" are either directed at another student or students; are severe, persistent, or pervasive; or have the effect of substantially interfering with a student's education, creating a threatening environment, or substantially disrupting school operation. Citation: H.B. 1067, 2008: 24 Pennsylvania Statutes §1303.1-A
Rhode Island		Prohibits "harassment, intimidation or bullying" through any "intentional written, electronic, verbal or physical act or threat of a physical act that" that a reasonable person should know will harm another student, damage another student's property, place another student in reasonable fear of harm to the student's person or damage to the student's property. Requires school districts to develop policies on harassment, intimidation or bullying. Citation: S. 2012, 2008: General Laws §16-21-26
South Dakota	Requires schools to equip computers with filtering software or to adopt policies to restrict minors from access to obscene materials. Citation: S.D. Codified Laws Ann. § 22-24-55 to 59	
South Carolina	Requires publicly funded libraries and public school libraries to adopt policies intended to reduce the ability of the user to access websites displaying obscene material. Also establishes a pilot program to evaluate the use of filtering software in libraries. Citation: S.C. Code Ann. § 10-1-205 to -206	Requires school systems to develop policies prohibiting bullying "at school." Bullying extends to communication through electronic means. Citation: H.B. 3573, 2006: South Carolina Code §59-63-120, §59-63-140

State Laws Pertaining to Filtering and Cyber-bullying

State	Internet Filtering Laws in Schools	Cyber-bullying
Tennessee	Requires the development of acceptable Internet use policies for public and private schools to protect children from certain online material. Citation: Tenn. Code § 49-1-221	
Texas	Prohibits a public school or public library that provides a computer used for Internet access from eligibility for a Texas Infrastructure Fund loan or grant unless the school or library adopts an Internet safety policy protecting children from access to obscene materials. Citation: Texas Ed. Code Ann. §§ 32.201 to -202, Texas Govt. Code Ann. §441.1385	

Sources: Children and the Internet: Laws Relating to Filtering, Blocking and Usage Policies in Schools and Libraries, National Conference of State Legislature, http://www.ncsl.org/default.aspx?tabid=13491
State Policies on School Cyberbullying, First Amendment Center, http://www.firstamendmentcenter.org/PDF/cyberbullying_policies.pdf

Note: Summaries state laws as of October, 2010

Bibliography

Barrington Public School District. (2001). *Policy Manual: Instruction.* Retrieved January 31, 2011 from http://www.barrington220.org/211410101992724577/lib/211410101992724577/_files/SECTION6.pdf

Bellingham Public Schools. (2002). *Board Policy: Student Access to Networked Information Resources.* Retrieved January 31, 2010 from http://bellinghamschools.org/department-owner/school-board/2313policy

Bosco, J. Salpeter, J. Mahon-Santos, A. (Summer 2010) *Web 2.0 as a Force for School Transformation: A Tale of Six Districts.* Consortium for School Networking. Vol.8, Issue 2. Retrieved January 31, 2010 from http://www.cosn.org/Portals/7/docs/compendium/2010/Executive%20Summary/CoSN-2010_CMPND-Vol8_Isu4-ExSmry_v3.pdf

Broward County Schools is website that includes all the information regarding the Broward County Schools (http://www.browardschools.com/).

City of Portsmouth School Department (2010). *AUP Policy.* Retrieved January 31, 2010 from http://www.cityofportsmouth.com/School/policy/AUPformsgrK-5.pdf

Cyber Security for the Digital District this website provides information and tools to help school districts protect their networks, and to assist them in using technology for teaching and learning. (http://www.cosn.org/Initiatives/CyberSecurity/tabid/5240/Default.aspx)

DeLisio, E. (2007). *Crafting A Workable Cell Phone Policy.* Education World. Retrieved January 31, 2010 from http://www.educationworld.com/a_admin/admin/admin393.shtml

Domenech, D. (2009, October). *Harnessing Kids' Tech Fascination.* The School Administrator, Number 9, Vol. 66. Retrieved January 31, 2010 from http://www.aasa.org/SchoolAdministratorArticle.aspx?id=6884

Duxbury Public Schools. (2010) *Internet Connectivity and Technology Tools Duxbury Public Schools Acceptable Use Guidelines.* Retrieved January 31, 2010 from http://www.duxbury.k12.ma.us/documents/AUG5-12-2010.pdf

Edina Public Schools. (2010). *Policy 634 Education Programs: Electronic Technologies Acceptable Use.* Retrieved January 31, 2010 from http://www.edina.k12.mn.us/district/board/edinabpm/600/634.pdf

E-Rate Central. (2001). *Children's Internet Protection Act. Retrieved——, from* http://www.e-ratecentral.com/CIPA/Childrens_Internet_Protection_Act.pdf

eSchool News. (2010, September). *Schools still conflicted over Web 2.0 tools* . Retrieved January 31, 2010 from http://www.eschoolnews.com/2010/09/28/schools-still-conflicted-over-web-2-0-tools/

Fairfax County Schools. (2010). *Student Responsibilities and Rights Grades K-12* Retrieved January 31, 2010 from http://www.fcps.edu/dss/ips/ssaw/SRNR/2010-11-SRR.pdf

Littleton Public Schools. (2010)). *Educational Technology Advisory Committee.* Retrieved —-, from http://www.littletonpublicschools.net/Default.aspx?tabid=295
First Amendment Center. (2010) *State Policies on School Cyberbullying.* Retrieved January 31, 2011 http://www.firstamendmentcenter.org/PDF/cyberbullying_policies.pdf

Maine International Center for Digital Learning. Provides a comprehensive document for use in developing an AUP. http://www.micdl.org/attachments/131

Moyle, K. (2009). *Varying Approaches to Internet Safety.* University of Canberra. Retrieved January 31, 2010 from http://www.cosn.org/Portals/7/docs/Web%202.0/Varying%20Approaches%20to%20Internet%20Safety.pdf

Palfrey, J., Gasser, U., boyd, d. (2010). *Response to FCC Notice of Inquiry 0994: Empowering Parents and Protecting Children in an Evolving Media Landscape.* Retrieved January 31, 2010 from http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Palfrey_Gasser_boyd_response_to_FCC_NOI_09-94_Feb2010.pdf

National Association of State Boards of Education (2009). *State School Healthy Policy Database.* Retrieved January 31, 2010 from http://nasbe.org/healthy_schools/hs/bytopics.php?topicid=3131&catExpand=acdnbtm_catC

National Conference of State Legislature (2011) Children and the Internet: Laws Relating to Filtering, Blocking and Usage Policies in Schools and Libraries, Retrieved January 31, 2011 from http://www.ncsl.org/default.aspx?tabid=13491

National Telecommunications and Information Administration. (2008). *Broadband Data Services Improvement.* Retrieved January 31, 2010 from http://www.ntia.doc.gov/advisory/onlinesafety/BroadbandData_PublicLaw110-385.pdf

New Canaan School District. (2008). *New Canaan Public Schools has adopted a new Acceptable Use Policy.* Retrieved January 31, 2010 from http://www2.newcanaan.k12.ct.us/education/page/download.php?fileinfo=TkNQU19BVVBfR3VpZGVsaW5lcy1SZXZpc2VkX0p1bHlfMjAwOC5wZGY6Ojovd3d3Ny9zY2hvb2xzL2N0L25ldy9pbWFnZXMvYXR0YWNoLzQ2MzIvMjQxOTBfNDYzMl9hdHRhY2hfMTgzNS5wZGY=

New Haven Public Schools. (2010). *Student Parent Handbook 2010-2011.* Retrieved January 31, 2010 from http://www.nhps.net/sites/default/files/10_MAY_21_SPH_ENG_no_withdrawl.pdf

Quillen, I. (October, 2010). *Schools Open Doors to Students' Mobile Device.* Education Week, Educational Directions. Retrieved January 31, 2010 from http://www.edweek.org/dd/articles/2010/10/20/01mobile.h04.html

Scrogan, L. (2007, August –September). *AUPs in a Web 2.0 World.* EdTech Magazine. Retrieved January 31, 2010 from http://www.edtechmag.com/k12/issues/august-september-2007/aups-in-a-web-2.0.html

Social Media Guidelines for Schools a wiki for collaboration on developing social media guidelines for schools. (http://socialmediaguidelines.pbworks.com/w/page/17050879/FrontPage)

State of Washington Department of Public Instruction. (2010). *Internet Safety Training Programs & Policy/AUP.* Retrieved January 31, 2010 from http://www.k12.wa.us/EdTech/InternetSafety/default.aspx

Springfield Public Schools. *Acceptable Use Policy.* Retrieved January 31, 2010 from http://www.sps.springfield.ma.us/schoolsites/central/students/pdf/internet_policy.pdf

Von Dobeneck, M. (2010, November). *Area School Reconsider Cell Phone Policies.* Patriot News. Retrieved January 31, 2010 from http://www.pennlive.com/midstate/index.ssf/2010/11/area_schools_reconsider_cell_p.html

Wang, A. (2010, October). Dysart Unified School District Takes a New Look at Old Cell Phone Policy. The Arizona Republic. Retrieved January 31, 2010 from http://www.dysart.org/Departments/CommunityRelations/articles/articles/2010-2011/Republic/10.15.10_Dysart_takes_new_look_at_old_cellphone_policy.pdf

Warwick School District is a website which contains the Warwick School District policy on cyber-bullying and related matters. (http://www.warwick.k12.pa.us/orgmodule.php?deptid=107&schoolid=0007&mid=248http://www.warwick.k12.pa.us/orgmodule.php?deptid=107&schoolid=0007&mid=248)