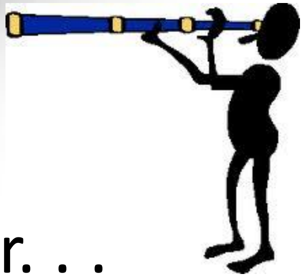
AUP’s & the New World

The “New World” Challenge

In this corner . . .

The need to give students access to the extensive resources on the Internet for learning and teaching.

VS.



In the other corner. . .

The need to protect students from dangerous and inappropriate material on the Internet.

How do we provide access?

“**Old World**”

- We provided the tools
  - Labs, carts, laptops
- Curriculum was text-based
- We had the “power” to manage the tools and access.

“**New World**”

- Engaging curriculum & authentic projects
  - Videos, publications, flipping classroom, digital textbooks,
- Expanded equipment
  - Computer labs, one-to-one, mobile carts
- Email, blogs, wikis, Google Docs,
- Netbooks, iPads, smart phones,
- Wireless throughout campus
- BYOD (with their own wireless plan!)

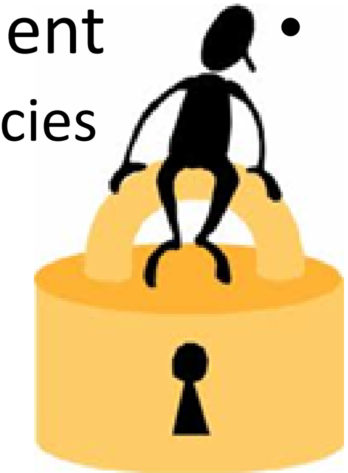
How do we protect kids?

“Old World”

- Education
  - Technology standards require teaching cyber safety.
- Filters
  - Tools to block and filter access to harmful sites.
- Policies & enforcement
  - Acceptable Use Policies (AUP).

“New World”

- Education
  - Technology standards require teaching *Digital Citizenship.*
- Filters
  - Need to change to be flexible and mobile.
- Policies & enforcement
  - Evolving into Respectful/ Appropriate Use Policies.



In the past, we focused on . . .

- The Children's Internet Protection Act (CIPA) is a federal law. The Children's Internet Protection Act ("CIPA"), of 2000, requires any school, district and library that accepts federal technology funds MUST comply with certain Internet filtering & policy requirements.
- Schools and libraries that accept funds for Internet access and/or internal connection services must also meet the Internet safety policies of the Neighborhood Children's Internet Protection Act ("NCIPA") which addresses broader issues of electronic messaging, disclosure of personal information of minors, and unlawful online activities.
- The Protecting Children in the 21st Century Act, 2008, (a.k.a known as the Broadband Act) seeks to expand internet acce to underserved populations, but adds an additional Internet Safety Policy requirement covering the education of minors about appropriate online behavior.

Districts worried about

- Funding (eRate),
- Security,
- Resource Utilization,
- Disruption to instruction

. . . . So we had filtering and AUP’s

Now . . . Really muddy water

- We still have to worry about the old requirements (funding, security, resource utilization & disruption), but now Web 2.0 applications and mobile Internet devices have added new issues to the safety/access situation for schools.
- What happens on Facebook, Twitter, You Tube, etc.
- Family Educational *Rights* and *Privacy* Act (FERPA)
- Media coverage & Law Suits
- Loss of enrollment/ Perceptions concerns
- New Cyber Bullying Laws push school responsibility beyond the buildings.

We cannot “filter” our way through these waters.

So now . . .how do we protect kids?

- Filters
  - Tools now block and track access on mobile devices $$$.
- Education
  - Technology standards require teaching digital citizenship.
  - Parent Workshops
- Policies & enforcement
  - *Acceptable Use Policies (AUP)* growing into *Electronic Resources Policies (ERP)*.

Specific vs. General

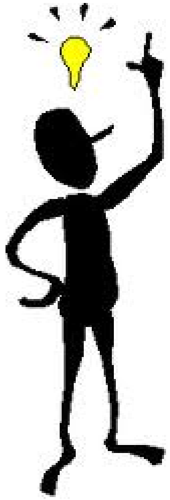
If you are going to permit web 2.0 tools and mobile devices, you have two options for drafting policy:

- Very specific -- Some districts state that the use of these tools is acceptable and go one to list specify what uses are inappropriate, unethical, or illegal.
- General -- Other districts believe that it is better to deal with acceptable and unacceptable use of these tools in a more generic manner, as “electronic” tools,” without tying to list specific types of applications.

Four Big Ideas Your Electronic Resources Policy

Washington State Office of Public Instruction

- Civic life has an expanding digital dimension that demands responsible engagement by individuals and groups.
- Responsible personal conduct within the *online* environment is no different than responsible personal conduct face-to-face.
- Individuals must protect personal safety online.
- There are long--lasting implications to publishing in the online environment.



Common Components of a Policy

- Link to mission and purpose
  - Link to overall code of conduct and stress focus on "educational purposes"
- Statement about scope
  - What services, devices, locations are covered by this policy
  - Include "no right to privacy"
- Acceptable/Responsible Use statement
  - Stress that access is for "educational purposes"
- Unacceptable use statement
  - Non-educational use parameters
  - Cyber bullying
  - Disruptions to instruction
- Violations/Sanctions/Consequences
  - Be careful about taking away access??
- A disclaimer absolving the school district from responsibility, under certain circumstances
- A form for teachers, parents and students to sign, indicating that they agree to abide by the AUP

Who should create your policy

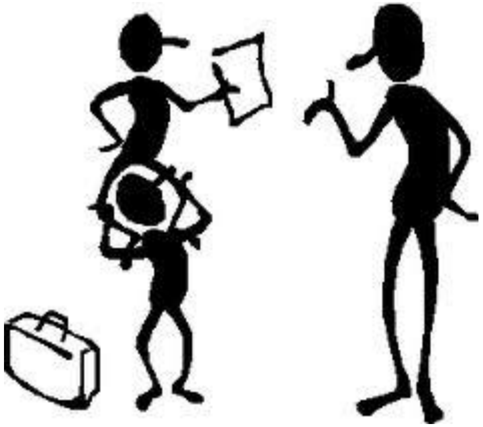
- One (or a small group of admin)
- Tech committee
- Policy board
- Parent representation
- Student representation
- Legal Review
- Board Reading, hearing and adoption

A thought about Cell Phones/Smart phones

- The prevalence of cell phones is driving school districts to revise their policy on cell phones & mobile devices.
- American Association of School Administrators are calling for less restrictive policies regarding smart phones.

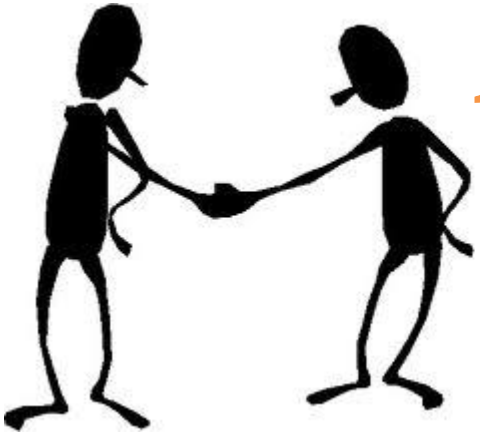
How do policies and AUP's change to accommodate these?

Reminder:
Not limited to students



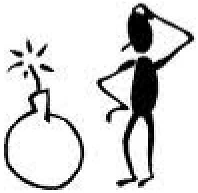
- What about staff use/access to tools
  - Non educational use during preps and lunch
  - File storage
- Use of their personal (outside) devices
  - Filtering logs (you tube, march madness, shopping sites,
- Rights to privacy
- FERPA (passwords)
- Copiers, phone calls, etc.
- Consistency
  - Kids cannot Facebook, text, talk on cell, etc. but teachers can???

One of the new Facebook Conundrums!



I can
“Friend”
who I want

No you
can’t!



Missouri's Amy Hestir Student Protection Act

- In July 2011, the state enacted the law, which modified a number of statutes designed to protect children from sex offenders.
- It was named after a woman who testified before the Missouri General Assembly, the state legislature, about sex abuse she experienced at the hands of a teacher when she was a teenager in the 1980s.
- The law included a ban on teachers communicating via any "non-work-related internet site [e.g., Facebook] that allows exclusive access with a current or former student."
- Passed unanimously by the legislature
- American Civil Liberties Union (ACLU) of Eastern Missouri sued the state on behalf of several Missouri teachers and the Missouri State Teachers Association filed a separate suit in state court.
- An injunction based on a First Amendment challenge temporarily barred enforcement of that provision of the law.
- Case is pending, but Missouri repealed the law and is currently revising it so it will stand up to the impending court challenge.

Do we now need a separate policy about how we communicate with students???

Michigan’s new Cyber Bullying Law

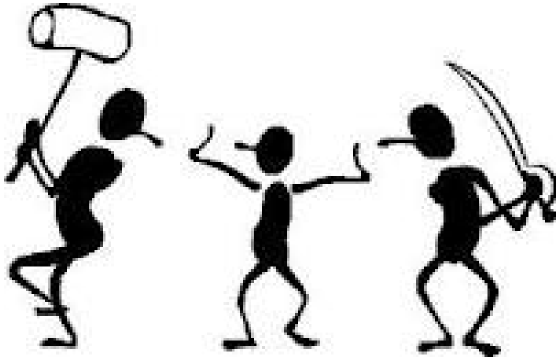
- ***Bullying/Harassment*** *:* HB4168 defines bullying as “any written, verbal, or physical act, or any electronic communication, that is intended or that a reasonable person would know is likely to harm 1 or more pupils either directly or indirectly by doing any of the following:

(1) Substantially interfering with educational opportunities, benefits, or programs of 1 or more pupils

(2) Adversely affecting the ability of a pupil to participate in or benefit from the school district’s or public school’s educational programs or activities by placing the pupil in reasonable fear of physical harm or by causing substantial emotional distress.

(3) Having an actual and substantial detrimental effect on a pupil’s physical or mental health.

(4) Causing substantial disruption in, or substantial interference with, the orderly operation of the school.”



HB4168 requires a policy prohibiting bullying ***at school***.

- Districts are required to hold at least on public hearing on the proposed policy. The policy must include:

(a) a statement prohibiting bullying of a pupil,

(b) a statement prohibiting retaliation or false accusation against a target of bullying, a witness, or another person with reliable information about an act of bullying,

(c) a provision indicating that all pupils are protected under the policy and that bullying is equally prohibited without regard to its subject matter or motivating animus,

(d) the identification by job title of school officials responsible for ensuring that the policy is implemented,

(e) A statement describing how the policy is to be publicized,

(f) a procedure for providing notification to the parent or legal guardian of a victim of bullying and the perpetrator,

(g) A procedure for reporting an act of bullying and for prompt investigation of a report, identifying either the principal their designee as the person responsible for the investigation,

(i) a procedure documenting any prohibited incident that is reported and a procedure to report all verified incidents of bullying and the resulting consequences to the board of the school district on an annual basis.

Additional recommendations for the policy are outlined in the legislation.

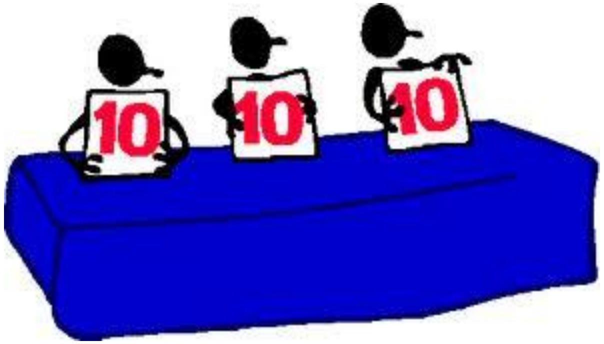
- The State Board of Education's Policies on Bullying (2011) recommends that schools should develop a plan designed to prevent bullying, and develop methods to react to bullying when it occurs, as an integral part of a district-wide safety and discipline plan.
- The state board also recommends that schools should institute an anti-bullying program incorporating the basic elements described in the policy, to promote a positive school atmosphere that fosters learning, and to create a fear-free school environment in the classroom, playground, and at school-sponsored activities.

Questions remain about . . . .

- How to best filter mobile devices
- Schools ability to address behavior that occurs outside of school,
- The blurring of the boundaries with new initiatives like the Seat-Time Waiver and online courses,
- Appropriate consequences
  - Can we take away access without impacting instruction now?

What do you think???

1. Definition
For the purpose of this policy, technology is defined as, but not limited to the following:
a. Instructional and staff workstations (both desktop and portable), printers, scanners and other peripherals;
b. Administrative staff workstations (both desktop and portable), printers, scanners and other peripherals;
c. Campus and departmental local area networks (both wired and wireless), including wiring, hubs, routers, transmitters/receivers and other devices;
d. Servers; including instructional lab servers, CD-ROM servers, video servers, file and print servers, database servers, internet proxy caching servers;
e. A Wide Area Network linking all SBBC sites into one countywide Intranet;
f. Telephone systems; including primary systems, integrated voice response/management systems, automatic dialing systems;
g. Learning resource management systems, including library automation systems;
h. Distance learning systems;
i. Video capturing, broadcast, receiving, and distribution systems;
j. Teleconferencing systems;
k. Application software packages which result in the creation and maintenance of an operational database;
l. Energy management and security monitoring systems;
m. Radio systems;
n. Office copier, imaging, and document management systems;
o. Paging systems;
p. Intercom; and
q. Facsimile systems.



Another sample . . .

Blogging/Podcasting. Uses of blogs, podcasts or other Web 2.0 tools are considered an extension of the classroom. Whether at home or in school, any speech that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, podcasts, or other Web 2.0 tools. Students using blogs, podcasts or other Web 2.0 tools are expected to act safely by keeping ALL personal information out of their posts. Comments made on school related blogs should follow the rules of online etiquette detailed above and will be monitored by school personnel. If inappropriate, they will be deleted. Never link to web sites from a blog without reading the entire article to make sure it is appropriate for a school setting.

Another sample . . .

- **Privacy.** E-mail is no more private than a postcard. Students and staff need to know that files stored on school computers are not private. Network and Internet access is provided as a tool for educational purposes only. The District has the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access including transmitted and received information. All information files are the property of the District and no user shall have any expectation of privacy regarding such files. Federal Law requires that all email sent and received be stored for a period of 'seven years'.

Another Sample . . .

- **Online Etiquette.** Follow the guidelines of accepted behaviors within the school handbook. Use appropriate language and graphics. Swearing, vulgarities, suggestive, obscene, belligerent, harassing, threatening or abusive language of any kind is not acceptable. Do not use school online access to make, distribute, or redistribute jokes, stories, cyber bullying, obscene material or material which is based on slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, or sexual orientation.

6. Acceptable use of Computer Network and Online Telecommunications

a. Rules

1. All use of telecommunication services and networks shall be consistent with the mission, goals, policies, and priorities of the school district.

2. Successful participation in a network requires that its users regard it as a shared resource and that members conduct themselves in a responsible, safe, ethical, and legal manner while using the network.

3. Staff and students who are exchanging communication with others outside the school are representing The School Board of Broward County, Florida, and should conduct themselves appropriately.

4. Use of these services shall be properly monitored and, to the extent reasonably possible, users of school sponsored telecommunication services and networks shall be protected from harassment or unsafe, unwanted, or unsolicited contact.

5. Upon receipt of written parental/guardian permission, students will be eligible to receive authorization to use computer network and online telecommunications from the appropriate supervisory unit (district office or school-based).

6. Technology owned or leased by the School Board shall not be used for advertising or otherwise promoting the interests of any commercial, religious, political or other non-district agency or organization except as permitted through board approved agreements, school board policies or state statutes with notification to the Associate Superintendent of Superintendent Support Division.

7. To implement the Acceptable Use provision of this policy, it is necessary that all users read and document in writing their understanding and willingness to comply with the "Code of Ethics for Computer Network and Online Telecommunications Users." (see below)

b. Code of Ethics for Computer Network and Online Telecommunications Users

1. All users are expected to read and understand the following privileges, rights, and responsibilities when using property or facilities (WAN, LAN, networks, Internet, Intranet, etc.) of Broward County public schools.

a. Use of computer network and online telecommunications is a privilege and must support teaching, learning, and research.

b. Students, parents, faculty, and staff in Broward County Public Schools will have access to network resources. Class assignments will have priority over other uses. Unlimited and open-ended use of telecommunications services or networks in terms of access time will be determined by each individual school principal, department administrator, or designee.

c. Authorized users shall be ultimately responsible for all activity under their account and password. Accounts shall be used only by the authorized user for the purposes specified.

d. Use of an identity or password other than the user's own is prohibited.

e. All network users shall adhere to the rules of copyright regarding software, information, and the attribution of authorship. Reposting communications of a personal nature without the author's permission or bulletin board messages without proper attribution is prohibited.

f. Any use of telecommunication services or networks for illegal, inappropriate, obscene, or pornographic purposes shall be prohibited. Illegal activities shall be defined as a violation of local, state, and/or federal laws. Inappropriate use shall be defined as a violation of the intended use of the district's mission, goals, policies, or procedures. Obscenity and/or pornography shall be defined as a violation of generally accepted social standards for use of a publicly owned and operated communication vehicle, and as defined by School Board policy.

g. All use of telecommunication services or networks for the promotion of an individual's personal or political agenda or commercial initiatives shall be prohibited.

h. Use of or engaging in offensive or inflammatory speech, profanity, or obscene language is not permitted at any time.

i. Hate mail, harassment, discriminatory remarks, and other antisocial behaviors are not permitted.

j. Users shall not intentionally spread computer viruses, vandalize the data, infiltrate systems, damage hardware or software, or in any way degrade or disrupt the use of the network.

k. Any attempts to degrade or disrupt system performance may be viewed as criminal activity in accordance with applicable state and federal law.

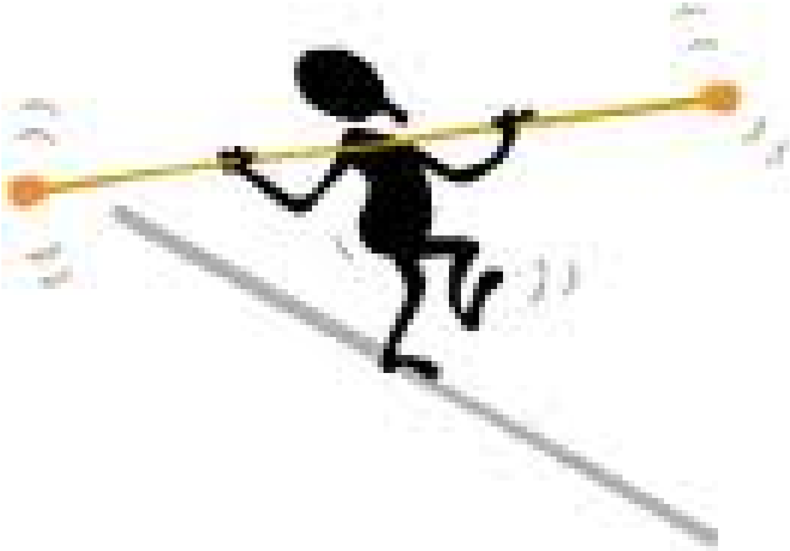
l. Files generated by district employees using School Board of Broward County property or facilities are the property of the School Board of Broward County and may be accessed by appropriate authorized system personnel.

2. Students and/or employees using School Board equipment or property, on-site or off-site, must conform to the requirements of this policy.

Key: Finding a Balance

The need to give students access to the extensive resources on the Internet for learning and teaching.

The need to protect students from dangerous and inappropriate material and behavior.



Resources

- NetCitizens, Monterey County Office of Education

http://sites.google.com/site/netcitizens/home/acceptable-use-policies

- CoSN – AUP resources

http://www.cosn.org/Initiatives/Web2/AUPGuide/tabid/8139/Default.aspx?utm_source=feb18_aupguide1&utm_medium=eblast&utm_campaign=guide#q1

- THE Journal article on Facebook & Schools

http://thejournal.com/articles/2012/03/02/online-safety.aspx?sc_lang=enCarol

- State of Washington Office of Education AUP suggestions

http://www.k12.wa.us/EdTech/InternetSafety/AcceptableUsePolicyInfo.aspx

Parents Guide to 21st Century Learning

- http://www.edutopia.org/parent-21st-century-learning-resource-guide