

TIPS FOR WEB SAFETY

Chicago SchoolTech: Jerry Crystal, Cherie Geide, Kaye Abight
New York SchoolTech: Sheila Gersh, Marykate Myer, Jan Rader

Tips for Creating and Enforcing AUPs

- Have teachers (and students) in on the process from the start—make the plan a team effort.
- All involved should sign the document.
- Get parents involved in other ways as well; keep them informed.
- Guidelines need to be very clear—as do penalties for violation.
- The person(s) responsible for enforcing the policies should be designated and empowered.
- Use English, not legalese.
- Don't reinvent the wheel. Be aware of AUPs that are available and working in other districts.
- Make sure the AUP is flexible.
- Post the AUP in a variety of places and be sure everyone is aware of it.
- Consider putting the information into the student handbook .
- The enforcement should be implemented consistently.
- Having students do a lot of their work in groups sometimes helps.

How To Avoid Overreacting

- If the rules and consequences are clear (see above) there should be less of a problem.
- Make it clear to students what they are to do if they access inappropriate material accidentally—including alerting the teacher, using the back button, turning off monitors, etc.
- Pay attention to body language—do students look as if they're trying to hide something?
- Stay calm and matter of fact.
- Explain and discuss when situations do arise.

Filtering Software—Whether and How to Choose It

- Some find a strong AUP, engaged teachers and supportive parents more effective than filtering.
- Firewalls are important.
- A well-paid technology person is needed who understands the network and can work well with students. Technical expertise and trust are both important.
- Appropriate assignments avoid much of the need for filtering.

- Given requirements for the E-rate and other funding, some protection is necessary.
- When shopping for filtering software, visit the Web sites of the top developers.
- Request demos/free trials to see which works best for you.

Other Tips for Supervising Student Use

- Make sure the monitors are visible to the teacher.
- Leave room for the teacher to walk around and work with groups.
- Have pre-selected sites for students to visit—either bookmarked or on a starter page.
- Use safe search engines (Yahooligans, Ask Jeeves for Kids, Kidsclick, Searchopolis, etc.)
- Internet access should always occur in a supervised setting.
- Student tech squads can play a role.
- When appropriate, use WebWhacker to grab sites or set up an “intranet” of Web sites.

Tips for Avoiding Stalkers and Other Predators

Make sure students know:

- Not to give out personal information about themselves or where they live
- Not to arrange to meet somebody they made contact with over the Internet (without adult supervision)
- About the dangers of joining unprotected chat rooms.
- To avoid sending pictures of themselves through e-mail.
- Not to fill out forms on the Internet without parent/teacher permission.
- Not to give out their passwords or let anybody use their e-mail accounts
- WHY these things are dangerous—with real examples (rather than just being told NEVER to do any of the above)

When posting information by/about students at a school Web site, consider:

- Posting any group photos without names.
- Using only first names on stories/bios and minimizing other personal information posted.
- Eliminating photos entirely or only using them at a protected intranet site.
- Providing information about the class as a whole rather than individual contributors.
- Password protecting your web site – giving out passwords to families only. This may seem extreme, but it can be effective.
- Not posting things like “student of the month” on the Web site.
- Looking at how other schools are successfully posting on the internet – what are they doing? Is it appropriate?

Other Do's and Don'ts to avoid putting students in jeopardy.

- Communicate the above safety rules to parents as well.
- Teachers should give students meaningful reasons for using the Net—and direct students to relevant and safe sites
- Encourage teachers to be active and involved.
- Report abuses to proper authorities.
- Be ready to deal with the reality that some students are going to go to inappropriate sites.
- Have a safe enough environment that students can tell you the situation and move on from there.
- Be flexible and plan well.
- Know the legislation

Helpful Tools And Resources For Web Safety

- **www.safekids.com**

Many relevant articles about Web safety, with lots of articles by Dr. Lawrence Magid, a reporter and child safety advocate. A well designed site with good information and links to other quality sites.

- **eSchool news August 1999 edition**

This particular issue talks about the filtering mandate and other legal issues for schools.

- **www.surfsafety.com**

Promotes an Internet safety book; author also does public speaking on internet safety.

- **www.erehwon.com/k12aup/**

A good site for internet AUP development. It has ideas and templates to help schools see what other schools are doing.

- **www.microweb.com/pepsite/Software/filters.html**

This site is an extensive list of software products that block, filter or monitor internet use.

- **www.sreb.org/Programs/ETCoop/edtech.html**

Info from the Southern Regional Education Board on AUPs

- **www.academicintegrity.org**

The Center for Academic Integrity provides a forum to identify, affirm, and promote the values of academic integrity among students. They list a variety of resources and links.

- **www.character.org/**

The Character Education Partnership (CEP) is a nonpartisan coalition of organizations and individuals dedicated to developing moral character and civic virtue in our nation's youth as one means of creating a more compassionate and responsible society.

- **www.plagiarism.com**

Now it is possible to prevent plagiarism by determining if a term paper has been copied from the Internet or from another class. Log into this site to check a student's work.

- **www.hifusion.com**

This is a FREE at home internet service that has built in filtering software as well as content and access that is grouped according to grade level or user.

- **<http://www.ftc.gov/bcp/online/edcams/kidzprivacy/>**

The Federal Trade Commission Website that directly deals with the privacy of kids information on the Internet. Many ideas for parents as well as links to resources.

- **www.cybercitizenpartners.org**

The Information Technology Association of America (ITAA) and the Department of Justice have created the Cybercitizen Partnership. The partnership is conducting a major

national campaign to educate, raise awareness and provide resources to empower concerned parents and others.

- **www.marymount.edu/ethics/cyberethics.html**

Link to the National Conference on Cyberethics being hosted by Marymount University and the Information Technology Association of America

- **www.missingkids.org**

A wealth of resources and safety guidelines for children and parents

- **www.tenet.edu/tenet-info/accept.html**

The Texas Education Network has a great supply of AUP's.

- **www.timeup.com**

An Internet safety (and Web hosting) site that explains the risks and benefits to Web surfing.

- **www.geocities.com/Athens/Stage/7519/**

Information on using "safe sites" developed by schools, colleges, universities, and other educational entities.

These three are on Internet Safety

Internet 101 - About Internet Safety <www2.famvid.com/i101/safe.html>

Internet Safety Site <www.willmar.com/iss/>

Coaching Kids for the Internet <www.iage.com>

To your Filtering Tools add:

Alfy Shield - A site suitable for preschool children. <www.alfy.com/>

Cybersitter Homepage

<www.solidoak.com>

A school edition of a filtering product. <www1.surfwatch.com/>

Edmark.com is a commercial site with free downloads, so you can try several out before you (or district) purchase.

<www.edmark.com>