

Writing an Acceptable Use Policy For Your School

By: Bruce Wentzell

Introduction

Students and staff need the opportunity to develop and practice life long learning skills. These skills are becoming more technologically oriented as society is communicating and providing information and services in new ways. Therefore, on-line services need to be integrated with existing learning and professional development activities.

In terms of improved educational and professional outcomes, when students and staff use on-line services they have a school without walls, with opportunities to:

- a) access and evaluate current up-to-the minute information;
- b) exchange cultural ideas, understanding, information;
- c) access and manipulate graphics, sound and videos;
- d) enhance literacy and writing, communication and information skills;
- e) download, collate, share and communicate relevant information;
- f) participate in global educational projects;
- g) participate in active learning;
- h) collaborate;
- i) work in self-managed learning environments;
- j) cater for diverse needs;
- k) broaden resource based learning tools;
- l) access experts and other professional resources.

The old saying, "If it sounds too good to be true, it probably is," is applicable to the Internet, which has its darker side. While most of the sites have the potential to be used in an educational setting, a small percentage can be objectionable for racial, sexist, political, sexual, or other reasons. These sites have received much publicity from the print and television media, who have left the impression among people who do not understand the true nature of the Internet that it is nothing but a collection of smut.

Many people do not understand that the Internet is an international linking of networks that is almost impossible to censor. One of the tools used to limit access to sites is filtering or blocking software. However, almost any student, given the time and the initiative, can learn to circumvent such software and find objectionable sites. In addition, software that blocks access to information can limit access to educationally legitimate sites. Another way of controlling content is limit access to certain categories of Internet services, such as newsgroups or electronic mail. However, if this course of action is pursued, students lose access to the educational benefits of these services. Another method of controlling access is to teach students responsible behavior and allow them access based on this behavior. This approach appears to be the wisest because it assists students in developing a sense of responsibility.

The Acceptable Use Policy (AUP) for Internet use is one of the most important documents a school will produce. Creating a workable AUP requires thoughtful research and planning. With

the current push for computer technology in the classroom, many educators and parents fear dangers that the uncensored Internet might hold for children: inappropriate or obscene words and images; violence; and people who pose an online threat. One strategy that many schools use to defuse such dangers is a student AUP for the Internet. Here we will learn about acceptable use policies and how to begin writing one for your school.

What is an Acceptable Use Policy?

Schools have dramatically increased their use of various computer networks and the Internet over the past decade. As a result, administrators, teachers, students, and parents have been forced to take steps to ensure that, when used responsibly, these resources are appropriate for use in school instruction. Many school districts, as well as individual schools, have established guidelines for the appropriate use of computer networks. Such a guideline is generally called an Acceptable Use Policy (AUP). An AUP is a written agreement signed by the students, their parents or guardians, and their teachers. The AUP outlines the terms, conditions, and rules of Internet use for the district or individual school.

Why Establish an Acceptable Use Policy?

The Internet is a large and unregulated global network. Increasingly, it is possible to find controversial material or behaviour on the Internet that some may see as offensive or inappropriate. This may include pornographic material or material with explicit sexual content, or unwanted attention or behaviour in private email. There are no foolproof technical solutions to completely prevent access to such material. Proactive policies help to establish a set of guidelines for the use of Internet access, and may help to establish or limit the extent of the school or staff's liability in the case of controversial or unwanted material being accessed through the transgression of such guidelines. In the absence of a clear and effective policy, overreaction or adverse publicity may endanger free and open access to the vast educational resources of the Internet.

An Acceptable Use Policy should...

1. Reflect the circumstances unique to your school or district and the electronic system used. It should clearly define what constitutes local responsible use of information networks.
2. Serve as a legal document. This means that you should get the school attorney to approve it before it is distributed for signing because:
 - a) It protects the school if an Internet-related incident occurs, such as an irate parent finding out their child has been visiting unauthorized sites.
 - b) It paves the way for prosecution of vandalism and hacking, should it occur.
3. Be complete. Your AUP should not just contain the rules of behaviour. It should include a statement concerning the school's position on Internet use.

4. Be adaptable. Since the Internet is constantly evolving, your AUP will need to be updated as new issues arise. Your AUP cannot anticipate every situation, so it should address the possibility that something could happen which is not outlined in the AUP.
5. Be unique to your school. Every school is different with respect to the degree of technology available to teachers and students, who has access to the network, who maintains the network, and the individuals teaching school personnel and/or students how to use the network.
6. Protect the students in your school. If your students follow the rules of the AUP their exposure to questionable materials should be minimized. In addition, it can protect them from dangerous net behaviour, such as giving out their names and addresses to strangers. An AUP also protects the parents. AUPs outline how their children will learn and be supervised with respect to Internet use. Parents have the option of accepting or rejecting the AUP, which either gives or refuses permission for their child to use the network at school. Finally, your AUP protects your school. If students, parents and teachers sign the AUP policy your school may not be held liable for irresponsible use of the Internet by students or staff members.

Components of an Acceptable Use Policy

The focus of an AUP should be on the responsible use of computer networks. Such networks include the Internet access (World Wide Web access, external e-mail, etc.) and Intranet access and transmitting of information (classroom networks, communications between classes within a school or district, library catalogue and database access, etc.). Most AUPs contain the following components:

1. A description of the instructional philosophies, strategies and goals to be supported by Internet access in schools.
2. A statement explaining the availability of computer networks to students and staff members in your school/schools.
3. A statement regarding the educational uses and advantages of the Internet in your school or district.
4. A statement explaining the responsibilities of educators, parents, and students when they use the Internet.
5. A code of conduct governing behaviour on the Internet.
6. A description of the consequences of violating the AUP.
7. A description of what constitutes acceptable and unacceptable use of the Internet.
8. A description of the rights of individuals using the networks in your school/district (e.g., right to free speech, right to privacy, etc.)
9. A disclaimer absolving the school district, under specific circumstances, from responsibility.

10. A statement that the AUP is in compliance with provincial and national telecommunication rules and regulations.
11. A form for teachers, parents, and students to sign indicating their agreement to abide by the AUP.

With this broad mission to fulfill within an AUP, most are usually packed with information.

Acceptable Use Policy—The Introduction

Suggested statements you may want to include in an AUP Introduction include some of the following:

- a) instructional philosophies and educational uses for using the Internet;
- b) constructive educational goals;
- c) advantages of using the Internet;
- d) disadvantages of using the Internet;
- e) a statement reminding users that Internet access and the use of computer networks is a privilege.

The school may also want to state in the introduction how it plans on restricting access to unacceptable materials through staff and student training, teacher supervision, network monitoring and filtering.

Acceptable Use Policy—The Definitions

Acceptable Use Guidelines need to be specific about what is acceptable or unacceptable. Vague terms or statements need to be defined. Words like Internet, Chat Rooms, Newsgroups, Email or World Wide Web may have no meaning for some parents. Besides defining what they mean, a description of how they would be used in a classroom setting needs to be included.

Statements like "inappropriate materials," "objectionable" or "inappropriate language" are too vague for students to determine what they should or should not do. Inappropriate materials might better be stated as "educationally inappropriate materials" or "inappropriate materials for classroom use." Inappropriate language could be rephrased as "language not appropriate for a classroom setting" or "language that is inappropriate in an educational setting." These types of statements need to be explained fully in an Acceptable and Unacceptable Use area of your guidelines. Itemized lists of what is acceptable or is unacceptable provide a better guideline for students and staff.

Acceptable Use Policy—The Policy Statement

A school might want to think about some of the following concerns when creating a policy for Internet use. This list is incomplete at best and is only intended as a resource to get you started.

- a) The kinds of access that students/staff will be allowed.

- b) How the school will restrict access to non-educational materials.
- c) How the Internet will be used in the classroom.
- d) A strict enforcement policy on downloading non-educational materials.
- e) Monitoring student use of the Internet.
- f) That Internet access is monitored and students email messages or computer storage areas are not guaranteed to be private.
- g) Network storage areas may be treated like school lockers.
- h) What online etiquette (Netiquette) is expected.
- i) A liability disclaimer statement.
- j) The school can not vouch for the accuracy of information on the school system or accessed through the school system.
- k) The school will not be responsible for any unauthorized purchase of products or services.
- l) A reminder that accessing the Internet through the schools network resources is a privilege, not a right.
- m) A statement about protecting the intellectual property rights (copyrights) of others.
- n) The school needs to explain the consequences of violating the policy.
- o) How the school addresses online privacy issues.

Acceptable Use Policy—Copyrights

A school could be held liable for copyrighted materials placed on the school web site. A copyright policy needs to make it clear that it is illegal to violate copyright laws. The schools policy to limit liability should include:

- a) A disclaimer that the school is not liable for student/staff violations of copyrighted material.
- b) Making copies of school owned or downloaded copyrighted commercial software, music, images or other materials is unacceptable.
- c) The school needs to establish a way to monitor all materials posted to the schools web site.
- d) Provide instruction for students/staff about copyrights and how to obtain permission to use copyrighted materials.

Acceptable Use Policy—Netiquette (Network and Email Etiquette)

Netiquette is a set of rules or manners for online behaviour. These rules or manners are not laws that the Internet community are forced to follow; they are the accepted behaviour the Internet community expects from its citizens. Many of the rules or manners have been established to address the limitations that are imposed on us by electronic communications.

Email messages and newsgroup messages lack the facial expressions, body language and tone of voice that we use when we communicate with each other face to face. The telephone at least conveys the tone of our voice. We can hear when the other person is kidding or being serious. Humorous and satirical remarks can take on a different quality without facial expressions and tone of voice. Misunderstandings can occur. Feelings can be hurt. The cleverly worded message fails to be read the way it was intended. Netiquette helps us avoid most of these misunderstandings.

Schools should include a list of the online behaviour they expect from students and staff in their AUP. These may include:

- a) Be polite!
- b) Do not send abusive or derogatory messages to anyone.
- c) Use appropriate language!
- d) Respect yours and others privacy!
- e) Do not give out personal information about yourself or other students/staff.
- f) Respect the rights of others!
- g) Use mixed case letters. It makes your messages easier to read. Typing an email message in all capital letters is viewed as shouting.
- h) Use emoticons (emotional icons), commonly referred to as “smileys,” to add a tone of voice or facial expression to your message. Smileys are used to soften those “tongue in cheek comments” meant to be funny but easily misinterpreted. For example, :-) means happy and :-(sad.
- i) Separate paragraphs with blank lines.
- j) Do not put anything in an email you do not want the world to read. Remember an email message can easily be forwarded to others.
- k) Proofread your email messages before sending them.
- l) Don't overuse acronyms and expressions. Not everyone is familiar with the meanings. Here are a few of the more commonly used ones: AFAIK—As Far As I Know, BTW—By The Way, HTH—Hope This Helps, IMO—In My Opinion, IOW—In Other Words, LOL—Laughing Out Loud, OTOH—On The Other Hand, VBG—Very Big Grin.

Acceptable Use Policy—The Privacy Issues

A privacy policy should address multiple issues of concerns. How student/staff personal emails and files will be treated. How staff will handle personal and confidential student information in emails and web pages. How students will handle personal information. Why protecting personal privacy information is a safety issue. How your personal information can be compromised by commercial Internet activities. Some of these safety rules that should be in an AUP are as follows:

- a) Don't meet with anyone you meet online without adult supervision.
- b) Don't open emails, files or click on web links in emails from people you don't know or you don't trust.
- c) Don't respond to email messages that are of a sexual nature, harassing, threatening, or make you feel uncomfortable. Immediately report these to a teacher or parent/guardian.
- d) Don't give out your password to anyone but your parents or guardian.
- e) Don't give out personal information about yourself, your family or others without getting appropriate permission.

Acceptable Use Policy—User Responsibility

Your policy can also outline that use of the organizations computing and information technology resources is granted on acceptance of the following specific responsibilities:

1. Use only those computing and information technology resources for which you have authorization.
2. Use computing and information technology resources only for their intended purpose.
3. Protect the access and integrity of computing and information technology resources.
4. Abide by applicable laws and school policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software.
5. Respect the privacy and personal rights of others.

In addition to a list of user responsibilities, a list of acceptable uses could include:

- a) Limited educational purposes;
- b) Class assignments;
- c) Career development activities;
- d) Educational research;
- e) Extra-curricular activities;
- f) To access reference materials;
- g) Communication activities;
- h) Personal communications.

Unacceptable uses could include any or all of the following listed items. This list of course is only provided as a resource. Each school will have to make a determination as to what are unacceptable uses that need to be outlined in their AUP.

- a) Sending or displaying offensive messages or pictures;
- b) Using obscene language;
- c) Giving personal information, such as complete name, phone number, address or identifiable photo, without permission from teacher and parent or guardian;
- d) Harassing, insulting or attacking others;
- e) Damaging or modifying computers, computer systems or computer networks;
- f) Violating copyright, local, provincial or federal laws;
- g) Using others' passwords;
- h) Trespassing in others' folders, work or files;
- i) Intentionally wasting limited resources;
- j) Employing the network for commercial purposes, financial gain, or fraud.

The consequences of violating the AUP also needs to be included. A school could list the consequences, but a better approach would be to list the AUP violation and the penalty.

- a) Violations may result in a loss of Internet access, detention, suspension, expulsion, or paying for damages.
- b) Illegal activities will be reported to the appropriate law enforcement agencies for investigation and prosecution.
- c) It might be found appropriate for violators to have to pay for misusing the schools network resources and equipment.

- d) Misusing printer privileges could result in a misuse fee to recover the cost of paper, toner and printer maintenance.

It is also advisable at this point to include a statement about how a student should report inadvertent accesses to unacceptable materials without being penalized.

Acceptable Use Policy—Consent Forms

The AUP should state that written parental consent is required before any student is given access to the Internet or to electronic mail. There needs to be a signature form for parents and students to sign indicating that they have read, understand and intend to abide by the school’s AUP. The form needs to be easy to understand and cover the unacceptable uses and penalties for misuse. It should state that students will be held accountable for violations of the AUP and that disciplinary action may be taken. Additionally, some schools are including a “sponsoring” teacher signature on each AUP. These sponsoring teachers are expected to provide specific instructions to their charges. The basic consent form will look something like this:

USER: I understand and will abide by the conditions, rules and Acceptable Use Policy. I further understand that any violation of the conditions, rules and Acceptable Use Policy is unethical and may constitute a criminal offence. Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken and/or appropriate legal action.

Date: User: Signature:

PARENT/GUARDIAN: As a parent/guardian of this student, I have read the Acceptable Use Policy. I understand that this access is designed for educational purposes. I also recognize that it is impossible for the school to restrict access to all controversial materials and I will not hold the school responsible for materials acquired on the network. Further, I accept full responsibility for supervision if and when my child’s use is not in a school setting. I hereby give permission to issue and account for my child and certify that the information contained on this form is correct.

Date: Parent/Guardian: Signature:

SPONSORING TEACHER: I have read the Acceptable Use Policy and agree to promote this agreement with the student. Because the student may use the network for individual work or in the context of another class, I cannot be held responsible for the student use of the network. As the sponsoring teacher I do agree to instruct the student on acceptable use of the network and proper network etiquette.

Date: Teacher: Signature:

Another preparative step used by many schools is an orientation session for students, parents/guardians, teachers, community members and/or others. This orientation and training happens before students are issued an account “login” name and password, or at the same time. The purpose of the session is to discuss concerns and issues addressed in the AUP, and to give preliminary and basic instructions for use of the account. Schools may also want to base student access to computer services on the successful completion of a “computer responsibility” test that

will help to ensure student understanding of the AUP guidelines. The test can be used as a tool to teach Internet etiquette, not a test to exclude anyone. If a student does not pass the test, the issues should be discussed and the test given again. Such a test could take on the following form:

Student Internet Test

True or False: (Circle the correct answer)

1. A student or teacher may not use the Internet to sell anything. T or F
2. The Internet is made up of many computer networks. T or F
3. It is OK to share your password with friends. T or F
4. Copyrighted material may be software, books, or files written by others. T or F
5. I can verbally abuse anyone using e-mail if I don't know the person I am writing to. T or F
6. "Download" means: receive a file from another computer. T or F
7. I should delete old files from my account to save space on the computer. T or F

Multiple Choice: (Circle the correct answers)

1. If you think that someone is using your password,
 - a) change your password
 - b) notify the teacher or network administrator
 - c) don't worry about it
 - d) a and b
2. When using e-mail, you
 - a) may send letters to anyone and say anything
 - b) may send e-mail for fun to anyone
 - c) never know who is reading your mail
 - d) must remember Acceptable Use Policy
 - e) c and d
3. If you need help,
 - a) ask the network operator or your teacher
 - b) look for help on the Internet
 - c) experiment
 - d) all of the above
 - e) none of the above
4. A computer "virus" is a problem. You should
 - a) check your disks for viruses
 - b) scan downloaded files for viruses
 - c) not worry about viruses because there are none on the Internet
 - d) not worry because the school will take care of it
 - e) a and b

Distribution of the Acceptable Use Policy

Schools will need to develop a distribution process in order to adequately inform all the involved parties. The following options might be considered once the AUP has been ratified:

- a) Copy to be included with school policy documentation and linked to the schools technology plan and web page.
- b) Inclusion in the staff handbook or as a staff handout.
- c) Copy distributed to parents/guardians through the school newsletter.
- d) Students rules included in a school diary or work books for secondary schools.
- e) Student rules displayed near all computers and in the Library or in other student areas.

Review of the Acceptable Use Policy

The AUP will need to be reviewed periodically. Experience has indicated that the period of review varies between schools, but that a review is usually appropriate at the end of the first year of implementation. After that, review of the policy is most likely to be included as part of the triennial technology planning process that each school should be initiating.

How Affective Is Your Acceptable Use Policy?

The following case studies reflect some of the typical situations that may arise in a school situation. Here you have the opportunity to consider your policies and school procedures ability to deal with them.

Case #1—Crude student message

A student sends an explicit sexual e-mail message to a teacher. Alarmed, the teacher forwards the message to the principal. What do you do?

Case #2—Unsupervised Use

A teacher extremely enthusiastic about the Internet encourages students to browse through the Internet during "free time." The teacher warns them to stay away from certain sites. One day a group of parents descend upon the principal to complain that their children have been browsing pornography in the back of the classroom while the teacher corrected papers in the front of the room. Your action?

Case #3—Restrictive software

The principal proposes software to restrict Internet access to select sites, preventing browsing and wandering. The librarian is asked to identify "safe" sites. The rest of the Internet will be "off bounds." How do you respond?

Case #4—Crude Teacher Message

A teacher sends a message to a buddy but accidentally sends copies to all staff members. The message contains several vulgar words. What do you do?

Case #5—Death or Stalking Threat

A teacher receives a death threat from a student. The principal is contacted, who brings the student and parents in for a conference. The student--a highly unlikely candidate for such behaviour--denies any knowledge or ownership of the message. What do you do?

Case #6—Overloading the System

A student constantly downloads very large files from the Internet and stores them on a computer. As a consequence, other users are having difficulty in finding storage space on the system for their files. What do you do?

Case #7—Breaking the Law

A teacher installs software onto the network that is personal property. It is unlicensed for the school. The teacher says that the students need access to this software but that the school will not or can not purchase it. What is your response?

One of the most important things to understand about these policies is that none of them are perfect. You will undoubtedly encounter situations that you could not have predicted. Still, these documents should not become instruments of paranoia. The vast majority of students will not do anything to cause difficulty for themselves or others on the network. Remember, the biggest problem that your students will find on the Internet stems from the cultural clash they will encounter between their familiar ways of talking to each other and the way people communicate in virtual environments.

Critiquing Your Acceptable Use Policy

As schools increasingly incorporate the Internet into their everyday curriculum, concerned administrators and parents have more opportunities to impose overzealous rules and limitations on teacher and student use of the Internet. Most schools are finding a common ground that both deals with the fears instilled in the public by news of isolated abuses, and also deals with the need to avoid censorship while introducing and teaching important technological and ethical concepts.

Various writers on AUP issues agree that in a pluralistic society there are, and should be, a very wide range of belief systems. This leads to a need for tolerance of a vast array of opinions and experiences. So, your AUP then, must serve as a way to moderate and guide users in situations where divergent beliefs come into conflict.

If you already have an AUP, have you asked how it came into existence? Unless the origin of the AUP is credible, it rests on a weak foundation. Students, teachers, parents, and administrators all need to have confidence that their concerns are well represented. People will not believe in your AUP unless it is, at least, well written, logical and internally consistent. It is much harder to respect and take seriously a form that shows inattention to communication details. Users should also have the right to know the possible consequences of misbehaviour without unnecessary waffling with the AUP itself.

Sometimes in AUPs the wording may include technical terms or vague generalities that make it difficult to determine what boundaries the policy defines. This type of AUP makes it possible

for authorities to revoke Internet privileges with little or no warning or explanation, leaving users confused and reluctant to explore the Internet. If the ground rules of your AUP are open to change, it should also say that any proposed changes will be announced before they are implemented. This way the users can always know the rules they are expected to follow.

Try to use simple terms in your AUP. A useful AUP will be understandable rather than intimidating to its users. Clearly defining what you will be punished for is also important. However, let the punishment fit the crime. Your AUP needs to acknowledge the human rights of student computer network users. The student's right to privacy is always mentioned. As well, all attempts should be made to educate students on how to respond to troublesome expressions and displays on the Internet if they occur.

It is just human nature to fear and protect against something we don't understand. But to many, the Internet has the same risks found everyday on television, printed in your local newspaper, or delivered to your mailbox. So the basic goal of a school's AUP is for students to attain self-control. As students mature, we as educators begin to rely less and less upon physical barriers, trying to teach them to respect boundary lines and values without being tied down, locked in or physically blocked from entry. We expect students to begin exercising judgment and restraint. We hope and expect that students will begin to adopt certain values as their own.

We are going to have to teach the children well. The locus of control is going to have to be in their heads and hearts, not in the laws or machines that make information so imperviously available. Before we let students loose on the Internet, they need to have a solid moral grounding and some common sense. A well developed AUP goes a long way to fulfilling these ideals.

Finally, as technology continues to advance we need different approaches to AUPs, because students are now increasingly required to participate in an Internet curriculum. Until quite recently, voluntary initiative was the basis of educational involvement in the Internet. But now there may be less personal choice available to students, and perhaps your AUP will need to be adjusted for this new reality. We need to continue to take a look at why and how we write and implement AUPs to ensure the successful use of the Internet for learning.

Conclusion

Writing and implementing an appropriate AUP for your school will go some way towards effectively managing user Internet access. However, it is not a general panacea and needs to be a component of your overall security and management procedures. The simple fact that you have an Internet AUP will make users aware that they do not have carte blanche when they are online and that they are ultimately responsible for their actions.

If you haven't got an Internet AUP then don't put it off, do something now. You should formulate and implement even the most basic policy before it is too late.

Sample Acceptable Use Policies

In writing your AUP, take advantage of what others have learned about drafting and implementing a policy. Visit Internet sites that have example or actual AUPs, talk with people, get ideas from people who have already implemented these plans, and don't be afraid to get interested parties together to resolve issues or solve problems. Reviewing AUPs from other schools and school districts may help to see how others have organized and written AUPs. Many of these examples may be used as a template to create an AUP for your own school or district. Remember, however, that your AUP should represent your school's or district's philosophy and needs regarding the use of the computer networks to which you have access.

Acceptable Use Policies: (December 1994-January 1995) Defining What's Allowed Online, and What's Not. Classroom Connect. [On-line]. Available <http://www.wentworth.com/classroom/aup.htm>

Armadillo's Rice University WWW Server: Acceptable Use Policies. The Texas Studies Gopher provides extensive links of resources for developing AUPs, including the Houston Independent School District's Acceptable Use Policy, a sample AUP form in English, and a sample AUP form in Spanish. <http://www.rice.edu/armadillo/acceptable.html>

Bellingham Public Schools offers students access to the district computer network for both electronic mail and the Internet to enable them to explore thousands of libraries, databases, and bulletin boards while exchanging messages with Internet users throughout the world. To gain access to e-mail and the Internet, all students need a signed Internet and Electronic Permission Form. This site contains both the District rules for Internet and e-mail and a copy of the permission form. <http://www.bham.wednet.edu/permis2.htm>

California Department of Education. (1994). Electronic Information Resources, Acceptable Use Policy, District Guidelines. [On-line]. Available <http://www.nmusd.k12.ca.us/Resources/Policies.html>

The CoVis Network Use Policy includes a template for you to use, and a paper on the topic of Acceptable Use Policies. http://www.covis.nwu.edu/CoVis_AUP.html

Chesapeake City Public Schools,
<http://www.pen.k12.va.us/go/VDOE/Technology/AUP/chesapeake.html>

School District #43, Coquitlam, British Columbia Internet Acceptable Use Policy,
<http://www.media-awareness.ca/eng/issues/internet/safety/hate/bcaup.htm>

The Eugene (OR) Public School District has developed a comprehensive site with guidelines for appropriate use, user application forms, student safety resources and technology resources at the district. Included amongst these resources is a pamphlet on keeping kids safe while they surf the Internet, Child Safety on the Information Highway. <http://www.4j.lane.edu/4jnet/>

K-12 Acceptable Use Policies. An excellent starting point by Nancy Willard at Internet Marketing Services for learning about Acceptable Use Policies, including templates for students, employees, guests, etc. <http://www.erhwon.com/k12aup/>

School District #42, Maple Ridge – Pitt Meadows, British Columbia.
<http://www.schdist42.bc.ca?AcceptableUse.html>

MO DESE Technology Network Project. The project CONNECT Website, which contains Acceptable Use Policies (AUPs) from a variety of school systems.
<http://services.dese.state.mo.us/projconnect.html>

Monroe County Community School Corporation, Bloomington, IN.
<http://www/mccsc.edu/policy.html>

New Horizon Governor's School For Science and Technology. (1994). Network Acceptable Use Policy. [On-line]. Available http://www.nhgs.tec.va.us/contributions/use_policy.html

Nova Scotia Department of Education and Culture Public School Programs' Internet Access and Use Policy – Code of Conduct, <http://doc-depot.ednet.ns.ca/internet/english/>

General Acceptable Use Policy Resources

American Library Association. (1991). Free Access to Libraries for Minors. [On-line]. Available <ftp://ftp.eff.org/pub/CAF/library/access.minors.ala>

An Incomplete Guide to the Internet. Especially for K-12 Teachers and Students compiled by the NCSA Education Group. December 1993, Chapter 2: Internet Etiquette, A basic guide to being considerate on the Internet. <http://www.ncsa.uiuc.edu/Edu/ICG/pt1.ch2.Etiquette.html>

Champelli, L. (1995). The Internet Advocate: a Web-based Resource Guide for Librarians and Educators Interested in Providing Youth Access to the Net. [On-line]. Available <http://silver.ucs.indiana.edu/~lchampel/netadv.htm#Part3>

Creating Board Policies for Student Use of the Internet. AUPs help to define acceptable behaviours by student and staff users of information systems, while Board policies take the matter much further tying those standards to the district's policies on student rights and responsibilities and a student's rights to privacy of freedom of speech. This article first appeared in From Now On, The Educational Technology Journal (vol.5, no. 7, May 1995).
<http://www.fromnowon.org/fnomay95.html>

Guidelines for School Internet Use: Ottawa Carleton Board of Education,
http://www.ocdsb.edu.on.ca/general_info/abbrv_accept_use_agree_form.htm

Internet Safety. This listing of links offers information on Acceptable Use Policies, including the article "Developing a School or District 'Acceptable Use Policy' for Student and Staff Access to the Internet," by Clancy J. Wolf (Ed. D). Wolf is the Internet Coordinator for 15 school districts

in northwestern Washington and has worked with many committees to develop AUPs.
<http://www.mcirel.org/products/tech/technology/safety.asp>

Intellectual Freedom: Road Kill on the Information Superhighway? This article by Janet Murray addresses both acceptable use policies for schools and the ALA's draft policy for electronic access to materials. <http://arlo.wilsonhs.pps.k12.or.us/ala.html>

Kinnaman, D. (1995, October 2). Critiquing Acceptable Use Policies. [Editorial]. [On-line]. Available <http://gnn.com/gnn/meta/edu/features/archive/aup.html>

Majid, L. J. (1994) Child Safety on the Information Highway. [Brochure]. National Center for Missing and Exploited Children and Interactive Services Association, Arlington, VA. [On-line]. Available <http://www.trms.ga.net/concerns/txt>

Netiquette. This Teacher magazine article by R.W. Burniske critiques the "Acceptable Use Policy for Technology" that Burniske's son brought home from school for a parent's signature. Burniske questions the appropriateness and usefulness of AUPs and suggests as an alternative a Cyberpilot's License program to address the skills, attitudes, and practices necessary to use the Internet. <http://www.edweek.org/tm/vol-09/05burnis.h09>

Rinaldi, A. M. (1992) The Net, User Guidelines and Netiquette. [On-line]. Available <http://www.fau.edu/rinaldi/net/index.htm>

Print Resources for Acceptable Use Policies

"The Internet and Acceptable Use Policies: What Schools Need To Know" The Eric Review. Vol. 14, Issue 1, Fall 1995, pp. 9-11.

"How To Write An Acceptable use Policy" Classroom Connect Oct 1995. pp.16-17.

"Another Look at Acceptable Use Policies" Technology Connection. Vol. 3(2) April 1996. pp. 23,25.

The Internet and Acceptable Use Policies: What Schools Need to Know (Kay Day and Lynne Schrum) The ERIC Review, Vol. 4. Issue 1, Fall 1995, pp. 9-11.

"Responsible Internet Use" Learning and Leading with Technology. Vol. 24 (6) March 1997. pp. 52-55.

Surfing in Shark-Infested Waters: Filtering Access to the Internet Larry Buchanan. MultiMedia Schools. March/April 1996. pp. 21-25.