

alt.sex:

Detour Off the Information Highway

by Frances Bryant Bradburn

Editor's Note: All information for this article has been gathered from a variety of sources on the Internet. The best resource that this author has found is gopher://chico.rice.edu:1170/11/More/Acceptable. While the resources on this list asked that quotes not be taken directly from their documents, this article would not have been possible without this information source.

Horror stories abound: Federal agents swarm an urban high school after a student threatens the President through the school's e-mail account; innocent children stumble upon an alternative lifestyle bulletin board while completing a homework assignment; parents discover bomb-making instructions downloaded from the Internet stashed under their son's mattress. Salacious stories, true or exaggerated, haunt all librarians as their publics clamor for more and more Internet access. Additionally, Congress is increasing librarians' worry quotient as it considers S. 314, the "Communications Decency Act of 1995," a bill that would "impose fines of up to \$100,000 and jail terms of up to two years upon those using telecommunications devices to send obscene, indecent or harassing material over the network."¹

But the truth of the matter is that issues such as these represent only a minuscule problem when we look at the overall value and potential of the Internet. Yet in order to sustain our patrons' access to the myriad resources available online, to protect ourselves and the institutions we represent, and to gain control over the next major censorship battleground, we librarians must be proactive. One of the prime

resources at our disposal as we take this proactive stance is the Acceptable Use Policy (AUP). An AUP is a statement of common understanding among Internet service providers and the people who use their service—a Code of Conduct, if you will. Every institution that offers Internet service should have an AUP in place *before* allowing access to its system. This protects not only the institution itself, but its Internet service provider as well.

Acceptable Use Policies are difficult for librarians, however, because they are fraught with intellectual freedom issues. AUPs often are designed for patron signature, especially in the case of Internet use by a minor. Additionally, real freedom of speech, freedom of expression, and privacy issues usually are addressed. The necessity of addressing institutional requirements for system security, as well as organizational and staff liability, is in direct competition with an individual's rights to free speech, privacy, and access to information. (ALA's Intellectual Freedom Committee will discuss its draft statement, "Access to Electronic Information, Services, and Networks: an Interpretation of the Library Bill of Rights," at this year's annual meeting in Chicago.) Then, too, some institutions limit Internet access to certain groups, classes, or even to certain hours. Equal access

issues often take a back seat to a library's financial or curricular issues.

Interestingly enough, K-12 schools may have fewer problems crafting AUPs than their other library counterparts because their prime focus for Internet use should be the curriculum. Additionally, individual schools or school systems already have in place procedures for dealing with many of the problems that surround Internet use. For instance, most schools have Codes of Conduct that address plagiarism, copyright violation, and even inappropriate language. Indeed, a school's field trip guidelines can apply to Internet use. After all, the Internet is one huge, virtual field trip, and students are representing their school out on the Internet as surely as if they were walking the halls of the state capitol. Most schools even require a parent's or guardian's signature for field trip participation. In short, a school's AUP can be based upon a variety of documents already in place—its selection policy, its codes of conduct, its field trip guidelines.

Public, special, and academic libraries tend to craft broader, less-defined AUPs than K-12 schools, often foregoing signature requirements, and spending less time on the moral and ethical issues of Internet use. All AUPs, however, regardless of institutional affilia-

tion, should contain these four components: mission statement, service provider, clientele, and disclaimer.

Mission Statement:

The mission statement, your statement of intent, is the most important part of an AUP. It is a library's *raison d'être*, the basis for all its service and, subsequently, the protection for both you and your service provider. The mission statement answers the questions: Why is your library providing Internet access? How is this resource being used? For schools, the traditional response is to support the school's curriculum, perhaps even a specific curriculum area such as social studies or science. For other libraries, it may be to supplement and enhance reference service, or to provide access to major academic collections in areas that have no local college or university. Pithy statements such as "To enhance the school's teaching and learning activities" and "To encourage open, scholarly communication and research" are often part of an institution's AUP.

Service Provider:

The disclaimer as to your institution's gateway is a part of any AUP. Whether your service provider is Nando, Interpath, or ECU, this information should be stated in your AUP. Additionally, review your service provider's AUP as you are writing your own. Check to see that your institution is in agreement with the gateway's AUP. It may be that your gateway has a policy of monitoring and reading all bulletin board or e-mail postings. Your institution's privacy disclaimers cannot be in conflict with your gateway's.

Clientele:

Also included within your AUP is a declaration as to whom you serve. Is Internet access only for staff reference librarians, students and faculty at your school alone, or the entire community? Spell this out within your AUP.

Disclaimers:

Most institutions believe it is important to remind their patrons that their access cannot be used for profit or extensive personal business. Additionally, libraries usually post a disclaimer that they cannot be responsible for loss of data, the content of general postings, or the down-time of the system. Some disclaimers even include the penalty(ies) for misuse. All these simply serve to

protect both the service provider and its gateway and, ultimately, everyone's use of the system.

There are myriad other issues to address as libraries craft AUPs. Some may be included with the AUP itself; others can be attached or distributed as expectations or information. Whatever the distribution decision, all these issues should be discussed at length and decisions made before Internet access, especially e-mail opportunities, is offered your staff and patrons.

One of the basic issues of electronic access to information, especially the e-mail provision of many Internet accounts, is privacy. All users need to understand up front that guaranteeing complete e-mail privacy is an impossibility. Any system operator can access e-mail and bulletin board postings on the system. Therefore, to guarantee privacy is heresy. We can, however, provide an institutional policy that deals with when and how we access individual patron information if the need should arise. Schools that insist on monitoring student e-mail activity as well as institutions that use a gateway that monitors postings should post this information in full view of their patrons.

One privacy issue that users tend to

The operative statement for Internet/e-mail use is "privacy, not anonymity." We have an obligation to protect our institutions and ourselves.

overlook is that of re-posting information. Whether as part of the AUP or provided as attached information, patrons should be reminded that re-posting another person's correspondence, whether to you personally or to a list, without the person's permission, is a violation of that person's privacy and may even infringe upon copyright.

Another issue is anonymity. The operative statement for Internet/e-mail use is "privacy, not anonymity." We have an obligation to protect our institutions and ourselves. Anonymous postings from our schools or libraries are equivalent to anonymous letters being sent from a local post office — not post office box, post office. Many institutions feel that in order to protect them-

selves, they must provide their patrons with some sort of identification whether it be a sign-in/sign-out sheet or individual e-mail addresses. That way, if a problem arises (the threat to the President or principal, copyright infringement) they will be able to follow up on the allegation.

Of course, this forces us to confront the freedom of expression issue immediately. Where do individual rights end and individual responsibility — not to mention general decency and common sense — begin? Most AUPs offer some type of network disclaimer that places responsibility for opinions and their subsequent airing directly on the user. Some may offer an additional caveat along the lines of, "We provide an intellectual climate of free and open discussion within the boundaries of appropriate school conduct." The morals and ethics of Internet use will be hotly debated, especially as the federal Communications Decency Act comes closer to a vote. All patrons deserve protection from harassment and unsolicited contact; all patrons ought to act decently and ethically in all their dealings, both electronic and otherwise. The bottom line, however, is that this conduct cannot be monitored effectively by the institution. Consequently, the education of patrons should be discussed and, ideally, provided by the institution that offers access.

Again, schools may be the most effective vehicle for this education, yet all providers should make an attempt to inform their public of expected behaviors when using this resource. Explaining about the common courtesies of checking and clearing e-mail regularly, not usurping the terminal when others are waiting, not altering electronic information, and not using another's password or entering another's mailbox should be a part of any patron's initial access to the Internet.

Finally, as distasteful as it may be, all AUPs or their accompanying support materials should address the consequences of AUP violation. Schools, colleges, and universities can refer to their discipline procedures and/or Codes of Conduct. Public libraries and special libraries may simply state loss of privileges as their "big stick." Whatever the penalty, patrons should know up front the expectations for use of this invaluable resource and the consequences of its misuse.

Reference

¹ *Net.News*, 1, 2 (March-April 1995): 2.



North Carolina Department of Public Instruction

NCDPI InfoWeb Acceptable Use Policy

The North Carolina Department of Public Instruction's InfoWeb is designed to offer easy access by the education community and general public to information about education in this state.

The Goal of NCDPI InfoWeb

The goal of NCDPI InfoWeb is to promote innovation and educational excellence in North Carolina. To achieve this, the network provides quality, equitable, and cost-effective information resources.

Use of NCDPI InfoWeb

Successful operation of the service requires that its users regard NCDPI InfoWeb as a shared resource, with the common purpose of advancing education in North Carolina.

The intent of the NCDPI InfoWeb Acceptable Use Policy is to ensure that all uses of NCDPI InfoWeb are consistent with the purposes of the agency. The policy does not attempt to detail all required behavior by its members. The following general guidelines are offered:

1. Any use of NCDPI InfoWeb for illegal purposes, or in support of illegal activities, is prohibited.
2. All use of NCDPI InfoWeb must be in support of education and research in North Carolina and consistent with the purposes of the agency.
3. Any use of NCDPI InfoWeb for commercial purposes is prohibited.
4. Any use of NCDPI InfoWeb for product advertisement or political lobbying is prohibited.
5. No use of NCDPI InfoWeb shall serve to disrupt the use of the network by other users.
6. All communications and information accessible via NCDPI InfoWeb should be assumed to be private property.
7. All NCDPI InfoWeb conferences and bulletin boards will be moderated.
8. Any NCDPI InfoWeb user's traffic that traverses another network may be subject to that network's acceptable use policy.
9. From time to time, the agency will make decisions on whether specific uses of NCDPI InfoWeb are consistent with this policy.

Last updated 1/31/95 ... dfw

QuickLinks

[Homepage] . [Outline] . [Curriculum] . [Internet]