

Network Working Group
Request for Comments: 1746
Category: Informational

B. Manning
ISI
D. Perkins
Houston ISD
December 1994

Ways to Define User Expectations

Status of this Memo

This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Abstract

This paper covers basic fundamentals that must be understood when one defines, interprets, or implements methods to control user expectations on or over the Internet.

1. Background

User agreements are a form of acceptable use policy (AUP) are an implicit part of internetworking since they place parameters on user expectation. They define the desired and expected behaviour of those who participate. Everyone has one, whether published or not. This applies to networks that provide transit paths for other networks as well as end sites and the individual users that use systems. A better understanding of an AUP, and how to formulate one seems to be increasingly important as the global net encompasses new environments as varied as K12 schools and real-time systems. AUP's are used to determine pricing, customer base, type and quality of service metrics, and a host of other provider services.

2. Components of an Agreement

In defining your particular agreement there are three areas that must be addressed. They are where you get service from, who your peers are, and whom you provide service to. A good understanding of these concepts will make or break the policies you formulate.

2.1 Where you get service from

Each entity gets its service from one or more other providers, either a level three service, such as IP transit, or a level two service, such as circuits. The provider of such services usually has an policy in the form of an agreement or contract specifying terms

and conditions of use. This forms the basis for the type of service offerings that you as an entity can provide. If you get service from several providers, all of them need to be considered in the formation of policy.

2.2 Who your peers are

Are your policies consistent with those offered by your peers? In many cases, the formation of policy will define who your peers are. It is important to clearly identify which areas you intend to reach and the community you wish to be a contributing, productive part of. Once this is clear, formulate policies along those lines.

2.3 Who you provide service to

It is required that you inform those who use your services just what your policies are. Without this information, it will be almost impossible for them to distinguish what to expect from your service offering. Without a clear policy it is possible that litigation may ensue. It is important to reflect community standards in the creation of policy.

3. Some Issues to consider

IP provided services can be complex. They comprise both information and communication. In the formulation of policy it is critical that the policy provide for security and access to information and communication while ensuring that the resource use does not overburden the system's capabilities. These conflicting demands must be analyzed and a synthesis arrived at. This hints a fourth component of an AUP, that it has a method to extract compliance. This is so site specific that further analysis will not be attempted here.

Some items that should be considered in the formation of policy are:

- | | |
|-------------------------|------------------------------|
| - privacy | - morals & ethics |
| - freedom of expression | - legal constraints |
| - safety | - harassment |
| - plagiarism | - resource utilization |
| - indemnification | - targeted areas of interest |
| - expected behaviours | - remedies and recourse |

This should not be considered as an exhaustive list but as pointers for those types of things to be considered when policy is formed.

4. Security Considerations

Security and Liability issues are not discussed in this memo.

5. Summary

User Agreements are here to stay. As the Interconnected mesh of networks grows, the choices presented to end-users mandate that provider/user expectations are clearly presented. Use of these guidelines will help create a clearer, better defined environment for everyone.

Authors' Addresses

Bill Manning
USC/Information Sciences Institute
4676 Admiralty Way
Marina del Rey, CA 90292

Phone: 822-1511
EMail: bmanning@isi.edu

Don Perkins
Instructional Media Services
Houston Independent School District
3830 Richmond
Houston, TX 77027

EMail: dperkins@tenet.edu

Example

For further reference on some acceptable use policies, see the following materials archived in Armadillo--The Texas Studies Gopher:

Name=Acceptable and Unacceptable Use of Net Resources (K12)
Type=1
Host=chico.rice.edu
Port=1170
Path=1/More/Acceptable

or:

<http://chico.rice.edu/armadillo>

If these resources are not available to you, you may want to review the attached policy and justification that is in use by an NSF sponsored project on K12 networking. It provides a view on the thinking process and actual Agreement that was worked out for this project.

The Internetworked School: A Policy for the Future*

Barry J. Fishman and Roy D. Pea School of Education and Social Policy
Northwestern University

Note:

The CoVis Network Use Policy itself appears as an appendix to this article.

Introduction

The next five years will radically change the ways that schools relate to the world around them as global computer networks--long the exclusive domain of higher education and private industry--link up to primary and secondary schools. The Internet, a network made up of many smaller contributing networks, represents a powerful educational resource unlike anything that precedes it. Its potential for education grows with the establishment of each new connection.

For the first time, schoolchildren have the means for simple, direct contact with millions of adults in a forum that masks their physical youth and presents them as virtual equals. However, just as the new kid in school has to learn new social codes and rituals to fit in, schools must learn some of the practices and etiquette of the Internet. Of course, the established denizens of the Internet will soon have some adjusting to do as well, with thousands (or millions)

of new kids knocking electronically at their doors. Since the Internet was not designed with children in mind, many potentially difficult issues must be discussed by both the education and the Internet communities.

This article presents a framework for thinking about some of the issues that are essential to making the initial encounter between schools and the Internet successful. It also presents an excerpt of a policy that embodies our approach to resolving those issues.

Expanding Access, Expanding Horizons

For roughly the past decade, schools increasingly have participated in specialized computer networks such as the NGS/TERC Kidsnetwork, the Intercultural Learning Network, and FidoNet, as well as for-profit services such as CompuServe, America Online, and Prodigy. The majority of these projects were conducted on networks, where teachers' or students' messages could not be read by anyone beyond a predetermined audience composed of other students and teachers. These projects made it possible for students and teachers to communicate with their peers in faraway places and pioneered some pedagogical uses of networks for computer-mediated communication and collaborative project work that will carry over to the Internet.

Internetworking, however, goes beyond proprietary systems by joining a vast number of distinct networks into one large network, the Internet. As individual schools and bulletin boards are connected to the Internet, the number of people and services within easy reach increases exponentially. By one estimate, there are currently 19 million users of the Internet, with an annual growth rate approaching 80 percent. Furthermore, some of the Internet's most powerful communication tools are specifically designed so that any of these millions of people could join any conversation. The network's true power comes from the synergy of many dispersed minds working together to solve problems and discuss issues, and there is little in the way of hierarchy or control of the discourse.

The schools' shift to internetworking systems involves critical technological, as well as pedagogical, issues. It requires a change in the school computing paradigm from centralized computing to distributed client-server systems, thus bringing about an administrative change in the nature of school computing. Many schools that currently have some kind of network access provide accounts only to teachers or administrators. Internetworking is fundamentally different--giving accounts, access, and therefore control directly to students.

There are numerous arguments for the pedagogical benefits of school internetworking. But what of the risks? What safety, liability, and, above all, educational concerns must be addressed before schools are ready to tap into the Internet? This policy is not intended as a document that sets limitations or restrictions. Rather, it is designed to facilitate and set guidelines for exploring and using the Internet as a tool for learning. The policy was written with the purpose and goals of the Internet as a background: support for open research and education in and among research and instructional institutions. The context for the policy was provided by the specific needs of a growing community of learners composed of students, teachers, scientists, and researchers. The networked environment must support collaboration and cooperation. Proper frameworks to support network navigation and information searching must be established. And because networks will continue to be a scarce educational resource for the foreseeable future, the policy also provides guidelines for maximizing the educational cost-benefit ratio for teachers and students.

Testbed for Change--The CoVis Project

Our framework for considering internetworking issues is a project currently being conducted at the School of Education and Social Policy at Northwestern University. The Learning Through Collaborative Visualization Project, CoVis, is designed to reconceptualize and reconfigure high school science education. CoVis is a networking testbed funded by the National Science Foundation (NSF). Its goal is to enable project-based approaches to science by using low- and medium-bandwidth networks to put students in direct contact with practicing scientists and scientific tools. In CoVis, we are working with the types of network connections we believe will be common in schools in the near future.

In the first phase of our project we are working with two Chicago-area schools, Evanston Township High School in Evanston and New Trier High School in Winnetka. CoVis is deployed in 12 classes at the two high schools, involving three teachers at each school. Approximately 300 students are involved in the project: 100 freshmen, 100 sophomores and juniors, and 100 seniors, all enrolled in either earth science or environmental science classes. Each classroom contains six Macintosh Quadra computers with audio/video conferencing units linked to an internal ethernet, which is linked to Northwestern's ethernet by a primary-rate Integrated Services Digital Network bridge for telecommunications using the public-switched network. Additional computers are available for Internet use in computer labs at each school.

The CoVis Network Community consists of students and teachers in CoVis classes, scientists who wish to collaborate on CoVis student projects, the researchers conducting the CoVis project, and other interested parties who are granted special accounts. In the CoVis classroom, each student is given an account that makes him or her a "full" member of the Internet community. This means two things: Each student has access to all Internet services with minimal mediation by teachers or other adults, and anybody with an Internet account can contact the students directly, again without mediation.

In addition to the standard Internet resources, which include electronic mail, listservs, Usenet news discussion groups, Telnet, gopher, and file transfer, CoVis makes it possible for students to communicate with peers and scientists via video and audio conference tools and remote screen-sharing technology for synchronous collaborative work. Therefore, the CoVis Network Use Policy goes beyond the needs of the typical low-bandwidth internetworked school.

As an NSF testbed, CoVis has the job of developing new frameworks for the use of internetworking. In seeking to understand problematic issues of networking, we turn both to other projects--Bolt Beranek and Newman's work with the Ralph Bunche computer-minischool in New York; AT&T's Learning Circles; and TERC's LabNet project--and to analogous situations extant in schools. Our attention thus is placed on the development of a policy to establish ground rules for the students who will be introduced to the Internet.

The Need for a Proactive Policy

Exciting or revolutionary educational programs too often are derailed. In the 1970s, Jerome Bruner's curriculum Man: A Course of Study (MACOS) was at the center of a political and ideological firestorm that prevented its implementation in many schools. The experience of the MACOS developers taught us that it makes sense to spend time in the initial stages of a project trying to determine what challenges might arise to an educational innovation in order to avoid, preempt, or co-opt them.

In March 1993, the Communications Policy Forum, a nonpartisan group of telecommunications stakeholders convened by the Electronic Frontier Foundation, met on the issues of Internet services for the K-12 educational community. The forum concluded that services should be provided only to schools that would indemnify the service providers. It also recommended that a warning statement be developed to advise schools of the presence of materials on the Internet that may be deemed inappropriate for minors.

We believe that it is not enough to devise a policy designed to protect schools and service providers, although our policy also speaks to those roles. In this policy designed to guide students through some of the social complexity presented by the Internet, we created guidelines to alert novice users of established expectations and practices. Because the Internet is somewhat anarchic in its daily commerce, it is necessary to define a safe local space, or identity, for a school network where students can feel like members of a supportive community. The goal of establishing the boundaries of our own community forms the framework of our policy.

Issues and Analogies

The kinds of issues posed by internetworking are not new. Similar issues have been debated by schools many times before, from creation science to dress codes. These concerns resurface in the availability of networked material that some parents, teachers, or students might find objectionable, pornographic, or otherwise inappropriate. Although the actual percentage of materials in this category is small, their mere presence draws plenty of media attention. Consider this lead-in to a story about graphic material that can be retrieved through the Internet, published in the Houston Chronicle in 1990:

"Westbury High School student Jeff Noxon's homework was rudely interrupted recently when he stumbled across the world's most sophisticated pornography ring....It was supported by taxes and brought into town by the brightest lights of higher education."

While some are shocked, an alternative interpretation might point out that in using a valuable resource provided by the local university, a high school student chose to view material that many (including regular Internet users) find objectionable. Educators must understand that, as a byproduct of introducing internetworking, schools likely will have to justify student use of network resources to a public that does not understand the medium or its utility to education. By seeking out analogous situations and applying them to the development of our network use policy, we believe it is possible to establish frameworks for responding to these challenges. We found several significant analogies.

* American Library Association (ALA). In considering information access issues, the most striking and informative analogy is to a remarkable set of documents built around the ALA's Library Bill of Rights of 1980. It is not farfetched to consider the Internet, at least in part, as a vast digital library. After all, the electronic database and information search tools it employs are rapidly becoming part of new school media centers, and many public and school libraries are beginning to offer some type of network access to their

patrons.

The ALA documents state, "Attempts to restrict access to library materials violate the basic tenets of the Library Bill of Rights." However, they add, what goes into the library collection should be chosen thoughtfully and with an eye toward instructional goals. School librarians are bound to devise collections that "are consistent with the philosophy, goals, and objectives of the school district," and they must "resist efforts by individuals to define what is appropriate for all students or teachers to read, view, or hear." Similarly, tools used to access the network must be designed to direct access to materials that support curricular concerns. Thus, the interface to the network embodies the notion of a library collection. In a school network policy, the "intent of the collection" should be clearly reflected in a statement of purpose for the network.

Directly addressing the information access needs of children, the ALA opposes attempts to limit access based on the age of a library user. "Librarians and governing bodies should maintain that parents--and only parents--have the right and the responsibility to restrict the access of their children--and only their children--to library resources," it states.

While we in the CoVis Project have some ability technologically to restrict what is in our Internet "collection," it is virtually impossible to prevent students from accessing materials whose presence we never anticipated while preserving the students' status as full members of the Internet community. In this way, the Internet is fundamentally different from a relatively static library collection. Following the lead of the ALA, however, we believe that the precise limits placed upon students' access cannot be formalized by the school policy. Instead, it is the students' responsibility to adhere to the standards set by their parents.

* American Society for Information Science (ASIS). The code of ethics of ASIS provides another informative analogy, this one speaking to issues of professionals' responsibilities to both individuals and society. Where individuals are concerned, information professionals--a designation we believe should be applied to teachers--must strive both to "protect each information user's and provider's right to privacy and confidentiality" and "respect an information provider's proprietary rights." With respect to society, information professionals should "serve the legitimate information needs of a large and complex society while at the same time being mindful of [the] individual's rights." They also should "resist efforts to censor publications."

The ASIS code speaks directly to issues of electronic mail privacy. We believe that students and teachers must feel certain that their communications are private. In many electronic mail systems currently used in schools, the teacher must act as an intermediary between the school and the outside world. When students are "full" members of the Internet, mail is sent directly to the outside world with no human mediation. As a rule, such communications should be private, and the network policy must make explicit any reasons for teachers or researchers to have access to message content. Users must be made aware of times and circumstances under which private mail may be monitored.

* Prodigy. Privacy in electronic mail communications seems like a straightforward issue--it is analogous to the U.S. mail. But what about network bulletin boards or Internet newsgroups? Posting a message in one of these public information exchanges may raise questions of freedom of expression among students and other network users, but no more than in any other public forum.

One approach to dealing with this issue was described in the Wall Street Journal's technology supplement of November 15, 1993. Prodigy, a dial-up bulletin-board service jointly owned by IBM and Sears, has a strict editorial policy for both its public forums and its members' private email exchanges. Prodigy employs editors who screen every message before it is posted, sometimes delaying posting by up to 40 hours. It also uses special software to screen messages for what it deems objectionable language. The result is a lowest-common-denominator approach to what is acceptable or unacceptable material.

This approach undervalues the maturity of Prodigy's users. In the CoVis classroom, we want to strive to develop students' maturity, and in order to learn these lessons, they must feel that their message content is under their own control. To let students know what level of behavior is expected of them, we are very clear about the use of offensive, obscene, or inflammatory language on the network. These guidelines are not unfamiliar to the students in CoVis, as their local school codes of conduct include the same admonitions. Offensive messages posted by students are not ejected from the network. However, students can lose their privileges on the network if they post such messages (a significant disincentive for CoVis students), and they are encouraged to post a retraction or apology once they understand why their message was problematic. These interventions are only initiated upon the complaint of another user, not as part of an explicit editorial policy.

* School Conduct Codes. Every school has a code of conduct for its students that details appropriate school behavior, outlines rights, and sets expectations for students. Because the CoVis Network is used

as part of a school activity, the school's code of conduct applies to network activities. Thus, we believe the network use policy should be an extension of the school's policies. An important part of the development of the CoVis Network use policy was a close reading of the participating high schools' codes of conduct. For example, at one of our high schools, special rules against vandalism of computer equipment and unauthorized access to information exist. These rules cover such important concepts as computer piracy, hacking, and other tampering with hardware or software. Both CoVis schools have codes warning students that use of harassing or abusive language is unacceptable, as is obscenity. At the same time, both high schools place a high value on students' right to freedom of expression and outline the dimensions of that right in some detail.

* **Field Trips.** All of the rules that apply to student conduct in school also apply when the students are off campus on field trips. The Internet offers many opportunities for virtual field trips to distant locations, and CoVis adds a new twist to this genre with the addition of full audio and video connections to remote locations. Students in the CoVis community will be able to "visit" the Exploratorium in San Francisco, directing a remote camera around the exhibit floor and engaging in conversations with guides and other museum visitors. It is important that students realize they act as ambassadors for their school in such encounters, and our policy states this explicitly. Currently, parental permission slips are required before students may take field trips. At one of our participating high schools, such slips are required even for "trips" within the school building. Is there a precedent for extending the concept of permission slips to the virtual field trip? We do not believe so, but we do recognize the importance of written information alerting parents to interesting or innovative school activities.

Beyond the Barriers

Barriers to internetworking in schools are being lowered every day, and soon electronic bulletin boards may be as familiar to the American classroom as blackboards. Educators are encouraged by continuing developments that make the Internet accessible to schools. This is accomplished in part through commercial networks such as America Online and Delphi and by the decreasing costs of modems and communications software. With the cooperation of nearby universities, dial-up Internet connections can now be obtained for an investment of under \$100 per existing computer.

Schools will find tremendous new opportunities for enhancing, extending, and rethinking the learning process with the advent of internetworking. But will they be ready to face the challenges? To date, schools have had little experience with advanced

telecommunications technologies. Many classrooms still lack even such basic tools as telephones. Given the general lack of communication even between classrooms in the same school, it will not be easy for schools to join in the fast-paced discourse of the Internet. The CoVis Project has taken a proactive stance toward the issues that internetworking raises for schools with the development of a network-use policy based upon the best lessons available. We invite feedback on our policy and offer it as a contribution to this exciting and rapidly developing area of educational technology.

Barry J. Fishman is a Ph.D. student in the Learning Sciences program of the Northwestern University School of Education and Social Policy. Roy D. Pea is Dean of the School and John Evans Professor of the Learning Sciences at Northwestern. They acknowledge the assistance of Laura D'Amico, Larry Friedman, Paul Reese, and Dick Ruopp in the preparation of this article. Their research is supported in part by National Science Foundation Grant MDR-9253462.

Margin Notes: Electronic versions of the original texts of American Library Association, American Society for Information Science, and Houston Chronicle documents can be found at FTP (file transfer protocol) address [ftp.eff.org](ftp://ftp.eff.org/pub/academic/library/directory), in the [pub/academic/library/directory](ftp://ftp.eff.org/pub/academic/library/directory).

The Communications Policy Forum meeting is reported on by Andrew Blau in the *EFFector* 5(4), also available from [ftp.eff.org](ftp://ftp.eff.org/pub/EFF/newsletters) in the [/pub/EFF/newsletters](ftp://ftp.eff.org/pub/EFF/newsletters) directory. Statistics about the Internet are available from [ftp.nisc.sri.com](ftp://ftp.nisc.sri.com), in the [/pub/zone](ftp://ftp.nisc.sri.com/pub/zone) directory. Both of these FTP sites can also be reached via gopher.

For further reading:

Roy Pea, "Distributed Multimedia Learning Environments: The Collaborative Visualization Project," *Communications of the ACM* (May 1993).

Denis Newman, Susan Bernstein, and Paul A. Reese, "Local Infrastructures for School Networking: Current Models and Prospects," Bolt Beranek and Newman Tech Report No. 7726 (1992).

Richard Ruopp, Shahaf Gal, Brian Drayton, and Meghan Pfister, *LabNet: Toward a Community of Practice* (Hillsdale, NJ: Erlbaum, 1993).

APPENDIX: THE COVIS NETWORK USE POLICY**A. Mission Statement**

The Learning Through Collaborative Visualization Project (CoVis) was established to explore project-enhanced science learning supported by advanced computing applications in a secondary school environment. As such, the computer network environment supported by the project (the CoVis Network) is designed to enhance the learning and teaching activities of the participating science classrooms at New Trier and Evanston Township High Schools. The term "network" in this document refers to a number of computers and other electronic tools that are connected to each other for the purpose of communication and data sharing. CoVis is a National Science Foundation (NSF) funded research project, and use of the network is therefore provided to allow the study of its impact on learning and teaching.

1. Purpose of the Internet

The Internet (a global network made up of many smaller contributing networks) and its services are intended to support open research and education in and among US research and instructional institutions, plus research arms of for-profit firms when engaged in open scholarly communication and research. Use for other purposes, e.g., for-profit activity or extensive personal business, is not acceptable.

2. Purpose of the CoVis Network

The purpose of the CoVis Network is to facilitate communications and collaboration between members of the CoVis community. Network use is primarily intended for the support of project work conducted for participating CoVis classes, and far less significantly for other purposes that students and teachers determine to be of educational value. The CoVis Network has limited resources, and CoVis classrooms have limited time available for network-supported teaching and learning activities. Any use of the network which adversely affects its operation in pursuit of teaching and learning or jeopardizes its use or performance for other community members is prohibited, and may result in the loss of network privileges.

B. Services Available on the CoVis Network

The CoVis Network consists of a variety of computing equipment, software, and network connections. This section describes the primary tools and services approved for use in the CoVis Network. Other tools may be used, but may not be supported by the system

administrators:

1. **Cruiser Videoconferencing.** Cruiser is a tool designed to allow video and audio connections between two people, each of whom must have a Cruiser station and access to the CoVis network. Cruiser conversations are private;
2. **Timbuktu Screen-Sharing.** Timbuktu is a commercial software product that allows a Macintosh user to view or control another Macintosh computer remotely (with the remote user's permission). This is designed to allow two or more people to work together over the CoVis Network. Timbuktu sessions are private;
3. **Collaborative Notebook.** The Notebook is a personal or group workspace designed to support project work in CoVis classrooms. Work done using the notebook may be either private or public, as designated by the user. Users should be careful to note whether they are working in a private or a public portion of the notebook.
4. **General-Use Internet Tools.** These include, but are not limited to, the following:
 - a) **Electronic Mail, or email.** Email is just like regular mail, except instead of paper, you use the computer. Email correspondence is considered private. The CoVis Project uses a program called "Eudora" for sending and receiving mail.
 - b) **Listservs.** A listserv is a means to broadcast an email message to many users for the purpose of maintaining a discussion list. Although listserv messages are transmitted via email, correspondence is public, so extra care should be used when participating. The program called "Eudora" would be used for participating in a listserv.
 - c) **Network News.** Netnews is a communications tool for large group discussion. Netnews is essentially similar to a listserv, except that it does not use email as the means of communication. Instead, you use software called a "news reader" to read and post messages to the appropriate groups. Newsgroups are very public, and should be used thoughtfully. The CoVis project employs a program called "NewsWatcher" for reading and posting news.
 - d) **File Transfer Protocol, or FTP.** File Transfer Protocol is a means of moving files between computers on the Internet. The CoVis project employs a program called "Fetch" for doing this.

e) Telnet. Telnet allows you to connect to other computers on the Internet, provided you know the machine's Internet address and appropriate password. All provisions of this document apply to members of the CoVis community while using remote computers via Telnet. The CoVis Project uses a program called "NCSA Telnet" for telnetting operations.

f) Gopher. Gopher is a means of navigating the Internet via a menu-driven or point-and-click interface to the computer. Gopher is a very convenient way to retrieve files and information from sources all around the globe. For most purposes, it may be considered an easier form of FTP and can be used to initiate Telnet sessions. The CoVis Project uses a program called "TurboGopher" for gopher searching.

C. Who is a member of the CoVis community?

All account holders on the CoVis Network will be granted access to all services the network offers. The following people may hold accounts on the CoVis Network:

1. Students. Students who are currently enrolled in a CoVis class will automatically be granted a network account upon agreement to the terms stated in this policy;
2. Teachers. Teachers of CoVis classes may hold accounts on the CoVis Network. Other teachers may apply for accounts;
3. Scientists. Scientists who wish to collaborate on student projects will be granted CoVis Network accounts. The exact nature of the account (i.e., which services are available) will depend on individual circumstances;
4. Researchers. The researchers conducting the CoVis project will hold accounts on the CoVis network;
5. Others. Anyone may request a special account on the CoVis network. These requests will be granted on a case-by-case basis, depending on need and resource availability.

Note: Except in special cases listed above, people from the larger Internet community are not part of the local CoVis community, and will probably be unaware of the existence of this policy. However, you should always treat people you "meet" on the network with respect, as if they were a part of your community.

D. Privileges and Rights of CoVis Network Community Members

Members of the CoVis community have certain network privileges and rights. These include:

1. **Privacy.** All members of the CoVis community have the right to privacy in their email, Cruiser, Timbuktu, and notebook communications when so designated by the user. However, if a user is believed to be in violation of the guidelines stated in this policy, a system administrator or teacher may need to gain access to private correspondence or files. An attempt will be made to notify the user of such inspections whenever possible. As CoVis is primarily a research project, researchers may periodically make requests to study or view correspondence and files, but confidentiality is ensured in such circumstances. Also, it is important that users recognize the fundamental differences between public (e.g., news) and private (e.g., email) forms of communication, and shape their content accordingly;

2. **Equal Access.** All members of the CoVis community will be granted free and equal access to as many network services as their technology allows. Exploration of the Internet is encouraged relative to the purposes of the CoVis Network;

3. **Safety.** To the greatest extent possible, members of the CoVis community will be protected from harassment or unwanted or unsolicited contact. Any community member who receives threatening or unwelcome communications should bring them to the attention of a system administrator or teacher. Users must, however, be aware that there are many services available on the Internet that could potentially be offensive to certain groups of users. The designers of the CoVis Network cannot eliminate access to all such services, nor could they even begin to identify them. Thus individual users must take responsibility for their own actions in navigating the network;

4. **Intellectual Freedom.** The CoVis Network must be a free and open forum for expression, including viewpoints that are strange, unorthodox, or unpopular. The network administrators will place no official sanctions upon the expression of personal opinion on the network. However, the poster of an opinion should be aware that other community members may be openly critical of such opinions. Occasionally, a message that you post may be met from outside the CoVis community with especially harsh criticism (a practice known as "flaming"). It is best not to respond to such attacks, unless you believe you are capable of a measured, rational reply. Personal attacks are not an acceptable use of the CoVis Network at any time. The CoVis Project does not officially

endorse any opinions stated on the network. Any statement of personal belief is implicitly understood to be representative of the author's individual point of view, and not that of the CoVis Network, its administrators, or the participating high schools.

E. Responsibilities of CoVis Network Community Members

With the rights and privileges of membership in the CoVis Network community come certain responsibilities. Users need to familiarize themselves with these responsibilities. Failure to follow them may result in the loss of network privileges. These responsibilities include:

1. Using appropriate language. Profanity or obscenity will not be tolerated on the CoVis Network. All community members should use language appropriate for school situations as indicated by school codes of conduct;
2. Avoiding offensive or inflammatory speech. Community members must respect the rights of others both in the local community and in the Internet at large. Personal attacks are an unacceptable use of the network. If you are the victim of a "flame," take time to respond rationally, and bring the incident to the attention of a teacher or system administrator;
3. Adhering to the rules of copyright. CoVis community members must respect all copyright issues regarding software, information, and attributions of authorship. The unauthorized copying or transfer of copyrighted materials may result in the loss of network privileges;
4. Re-posting personal communications without the original author's prior consent is prohibited. To do this is a violation of the author's privacy. However, all messages posted in a public forum such as newsgroups or listservs may be copied in subsequent communications, so long as proper attribution is given;
5. Use of the network for any illegal activities is prohibited. Illegal activities include tampering with computer hardware or software, unauthorized entry into computers, or knowledgeable vandalism or destruction of computer files. Such activity is considered a crime under state and federal law;
6. Avoid the knowing or inadvertent spread of computer viruses. "Computer viruses" are programs that have been developed as pranks, and can destroy valuable programs and data. To reduce the risk of spreading a computer virus, do not import files from unknown or disreputable sources. If you do obtain software or

files from remote sources, follow proper procedures to check for viruses before use. Deliberate attempts to degrade or disrupt system performance of the CoVis Network or any other computer system or network on the Internet by spreading computer viruses is considered criminal activity under state and federal law;

7. You have full responsibility for the use of your account. All violations of this policy that can be traced to an individual account name will be treated as the sole responsibility of the owner of that account. Under no conditions should you give your password to another user;

8. Impersonation is not permitted. Real names must be used, pseudonyms are not allowed;

9. Anonymity is not allowed on the CoVis Network. As an educational network, we believe that individuals must take responsibility for their actions and words;

10. Exemplary behavior is expected on 'virtual' field trips. When 'visiting' locations on the Internet or using the Cruiser or Timbuktu communication tools, CoVis community members must conduct themselves as representatives of both their respective schools and the CoVis community as a whole. Conduct that is in conflict with the responsibilities outlined in this document will be subject to loss of network privileges.

Note:

This article is reprinted with the express permission of TECHNOS: Quarterly for Education and Technology.

It originally appeared as: Fishman, B., and Pea, R.D. (1994). The internetworked school: A policy for the future. Technos: Quarterly of Education and Technology 3 (1), 22-26.