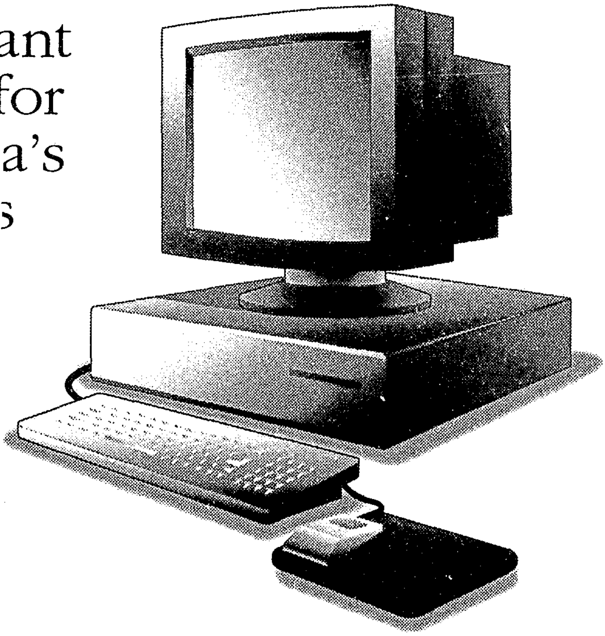
U.S. Department of Justice
Office of Justice Programs
*National Institute of Justice*

**NATIONAL INSTITUTE OF JUSTICE**
*Issues and Practices*

**DEPARTMENT OF EDUCATION**

# Ethical Use of Information Technologies in Education

Important Issues for
a's
s



# About the National Institute of Justice

The National Institute of Justice is the research and development agency of the U.S. Department of Justice, established to prevent and reduce crime and to improve the criminal justice system. Specific mandates established by Congress in the Omnibus Crime Control and Safe Streets Act of 1968, as amended, and the Anti-Drug Abuse Act of 1988 direct the National Institute of Justice to:

- *Sponsor special projects and research and development programs* that will improve and strengthen the criminal justice system and reduce or prevent crime.
- *Conduct national demonstration projects* that employ innovative or promising approaches for improving criminal justice.
- *Develop new technologies* to fight crime and improve criminal justice.
- *Evaluate the effectiveness of criminal justice programs* and identify programs that promise to be successful if continued or repeated.
- *Recommend actions* that can be taken by Federal, State, and local governments as well as private organizations to improve criminal justice.
- *Carry out research on criminal behavior.*
- *Develop new methods of crime prevention* and reduction of crime and delinquency.

The National Institute of Justice has a long history of accomplishments, including the following:

- Basic research on career criminals that led to development of special police and prosecutor units to deal with repeat offenders.
- Research that confirmed the link between drugs and crime.
- The research and development program that resulted in the creation of police body armor that has meant the difference between life and death to hundreds of police officers.
- Pioneering scientific advances such as the research and development of DNA analysis to positively identify suspects and eliminate the innocent from suspicion.
- The evaluation of innovative justice programs to determine what works, including drug enforcement, community policing, community anti-drug initiatives, prosecution of complex drug cases, drug testing throughout the criminal justice system, and user accountability programs.
- Creation of a corrections information-sharing system that enables State and local officials to exchange more efficient and cost-effective concepts and techniques for planning, financing, and constructing new prisons and jails.
- Operation of the world's largest criminal justice information clearinghouse, a resource used by State and local officials across the Nation and by criminal justice agencies in foreign countries.

The Institute Director, who is appointed by the President and confirmed by the Senate, establishes the Institute's objectives, guided by the priorities of the Department of Justice and the needs of the criminal justice field. The Institute actively solicits the views of criminal justice professionals to identify their most critical problems. Dedicated to the priorities of Federal, State, and local criminal justice agencies, research and development at the National Institute of Justice continues to search for answers to what works and why in the Nation's war on drugs and crime.

**U.S. Department of Justice**
Office of Justice Programs
*National Institute of Justice*

# Ethical Use of Information Technologies in Education: Important Issues for America's Schools

**by**
**Jay P. Sivin**
**Ellen R. Bialo**

May 1992

*Issues and Practices in Criminal Justice* is a publication of the National Institute of Justice. Designed for the criminal justice professional, each *Issues and Practices* report presents the program options and management issues in a topic area, based on a review of research and evaluation findings, operational experience, and expert opinion in the subject. The intent is to provide criminal justice managers and administrators with the information to make informed choices in planning, implementing , and improving programs and practice.

Prepared for the National Institute of Justice, U.S. Department of Justice, by the Institute for Law and Justice, Inc. under contract number OJP-91-C-005 Points of view or opinions stated in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice or the U.S. Department of Education. Authors are Jay P. Sivin and Ellen R. Bialo of Interactive Educational Systems Design (IESD), Inc. of New York, NY.

The Assistant Attorney General, Office of Justice Programs, establishes the policies and priorities, and manages and coordinates the activities of the Bureau of Justice Assistance, Bureau of Justice Statistics, National Institute of Justice, Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

**National Institute of Justice**
Charles B. DeWitt
*Director*

*Program Monitor*

Jonathan Budd
National Institute of Justice
Washington, D.C.

# Foreword

Plato posed the central ethics issue addressed in this publication in the *Republic*: suppose you had a ring which when you turned the stone, made you invisible. Why then should you act justly? The same question faces today's computer user who, with technology's aid, can effectively become invisible. The problem was ancient in Plato's time; the philosopher makes his point with the Ring of Gyges–already a legend in 400 B.C.

The ethical questions we face today are as old as the pyramids, and the circumstances as new as the latest piece of computer software. How do we best assure the just and effective use of the new technologies that are an increasingly vital part of both our personal and professional lives?

Preparing this Nation's youth to be productive and thoughtful adults, able to compete successfully in a global economy and to exercise the rights and responsibilities of citizenship, is a key objective of the President's National Education Goals and AMERICA 2000 education strategy. Achieving this objective will require educating students in the uses of computers and other new technologies which are opening career possibilities unheard of just a few years ago. The Nation's elementary and secondary schools are rising to the challenge. Computers are now part of the instructional program in the majority of American schools; and a significant percentage of students are already computer literate.

The increasing use and importance of computers has resulted in the rapid growth of such illegitimate practices as piracy, fraud, information destruction, and telecommunications abuse. Computer crime is generally on the rise, creating increasingly serious problems for law enforcement officials. Prevention through education in the responsible use of computers is an important part of the effort to reduce computer crime.

That is why the Department of Education and the Department of Justice have formed a partnership to promote school programs on the ethical uses of new technologies. This report, the first of the partnership between the Office for Educational Research and Improvement and the National Institute of Justice, is designed to assist schools in preparing a strategy to address technology-related ethical issues.

The ethical questions posed by our new technological circumstances are important ones–and many of them appear in shapes unfamiliar to teachers students alike. We believe that ethics issues related to the use of these technologies need to be addressed from kindergarten through graduation—and computer ethics education programs need to involve students, teachers, administrators, school board members, parents, and community and business leaders. The challenge is clear and the message is positive: computers are great tools when used responsibly.

Diane Ravitch
Assistant Secretary of Education
for Educational Research and
Improvement

Charles B. DeWitt
Director, National Institute of Justice

# Technology Ethics for Schools Advisory Panel

Virginia Baldau
Director
Research Applications and Training Division
National Institute of Justice

Sally Bowman
Director
Computer Learning Foundation

Jonathan Budd
Program Manager
Computer Crime
National Institute of Justice

Richard Hollinger
Department of Sociology
University of Florida

Kathleen M. Hurley
Education Marketing
IBM

Deborah Johnson
School of Humanities and Social Sciences
Rensselaer Polytechnic Institute

Larry Martin
Executive Secretary
Subcommittee for Automated Information System Security
National Security Agency

Jim Mecklenburger
Institute for the Transfer of Technology to Education
National School Board Association

Steve Purdy
Agent
Secret Service

Paul Resta, Ph.D.
Director
Learning Resource Center
University of Texas

Allen Schmieder
Director
Eisenhower National Program for Mathematics and Science Education
U.S. Department of Education

Connie Stout
Education Program Director
Division of Technology Development
Texas Education Agency

Gail Thackeray
Deputy County Attorney
Maricopa County Arizona

Cheryl Williams
Director
Technology Leadership Network
National School Board Association

Stanley Zenor
Executive Director
Association for Educational Communication and Technology

# Table of Contents

## Table of Contents (continued)

### List of Exhibits

# ETHICAL USE OF INFORMATION TECHNOLOGIES IN EDUCATION: IMPORTANT ISSUES FOR AMERICA'S SCHOOLS

Throughout the United States, educators are finding ways to use computers and related technologies to enhance student learning. However, as teachers and students become more experienced with educational technology, they are forced to deal with a variety of complex ethical and legal issues. Consider the following scenarios, based on instances that have occurred or could easily occur:

> In an elementary school where the budget for instructional supplies has been drastically cut, teachers are concerned that there is not enough money to purchase software for use with their students. A number of teachers make illegal copies of commercial, educational software programs, which they distribute to their colleagues.
>
> At a middle school where students are encouraged to practice writing skills by sending electronic mail (*e-mail*)[1] to one another over the school network, one student electronically sends an obscene story to several of his friends, who in turn circulate it widely over the network. When confronted by school authorities, the original student maintains that he has a right to send personal mail of any sort to his friends.
>
> A high school teacher sets up an *electronic bulletin board*, a system that allows students at different sites to communicate using computers and telephone lines.[2] Over time, a network of students learns how to use the bulletin board to pull off what the students consider to be "pranks." These abuses of the network include the distribution of stolen long distance telephone access codes and the introduction of a *virus*[3] program which destroys data on the system and eventually causes it to crash. Before reinstalling the bulletin board, the teacher and the students who have been assigned to run the system struggle with what rules to set for future users, how

to detect violators, and what actions to take to enforce the new rules.

A teacher shows her students how to combine text, graphics, video segments, digitized voice and music to create computerized multimedia presentations, which can then be transferred to videotape. The students capture music from audio CDs and use graphic images from a commercial graphics library and from books (using an image *scanner*) to create their videotapes. The teacher distributes copies of the videotape to colleagues from other schools. She worries that this distribution may be a violation of copyright law.

With help from *telecommunications* skills[4] learned at school, a student uses his home computer to gain unauthorized access to a nationwide credit history database and alters the data in some records. As a result, some credit-worthy consumers experience difficulty acquiring bank loans. When the student is caught by authorities, debate ensues in the community about the role the school should play in preventing future on-line abuse.

Students in a junior high English class are asked to keep a daily word processing diary. When one student is absent, another student accesses and reads her diary entries—entries that reveal extremely private details of her life. After the English teacher discovers this abuse, she approaches others on the faculty to discuss ways of defining and protecting private files on the network.

Situations like these are being encountered today across our nation. They are evidence that students and, in some cases, educators need both information and guidance concerning the legal and ethical implications of technology use. Unfortunately, few school systems have the policies and educational programs in place to address ethical issues as they relate to technology—issues such as: physical and intellectual property rights;[5] the right to privacy; and limitations on the right to free expression.

This time lag between the introduction of new technology and attempts to address its ethical implications is nothing new.[6] Other technological advances, such as nuclear energy and the automobile, were implemented in our society long before their responsible use was fully considered. Just as our nation's schools now offer driver education to encourage the responsible use of automobiles, our schools need to address responsible use of computers and related technologies as well.

This paper offers an overview of technology ethics issues for teachers, school administrators, and members of the community concerned about school policy. In this paper, we explore answers to the following questions:

- Why are technology ethics issues important for our society?
- How can information technology change what we think of as ethical behavior?
- Why do many students find the concept of intellectual property confusing?
- What can schools do to address these problems?

## THE CHALLENGE

Computer-related crime is a growing problem in our society. When criminal justice officials speak of computer-related crimes, they include fraudulent use of telephone services, use of computer networks to distribute stolen credit card numbers, embezzlement via computer, automated teller machine (ATM) fraud, unauthorized access to computer networks, tampering with electronically-stored records or programs (either directly or through programs such as viruses), and unauthorized copying or distribution of software (Conly, July 1989). Such crimes are costing American business a tremendous amount of money and adding to an already overloaded criminal justice system. (See Box 1 on the impact of these crimes.)

While the proportion of technology abuse committed by school-age children is presently small, there is concern about the adults that today's computer-literate children will become. In a recent conference on computer-related crime convened by the National Institute of Justice, there was consensus that:

> . . . given increased computer use in schools, the pool of potential abusers is growing substantially. . . . The nature of

the technology can invite abuse if users are not educated to understand the implications and consequences of their actions.[7]

## Box 1

## The Impact of Computer-Related Crime

Approximately one-fourth of Florida businesses responding to a recent survey reported having been the victim of a computer crime (Herig, 1989). A national survey found that 84 percent of the police chiefs in large, urban jurisdictions expected computer crime to have a serious impact on future workloads. Criminal justice professionals predict that computer abuse will steadily increase. (Conly and McEwen, January/February 1990).

Estimates of the financial losses due to technology abuse vary widely, depending on what forms of abuse are considered, and on how much underreporting by corporations is assumed. (Many companies are afraid of the financial impact when the public learns that their computer systems are insecure.) One recent report estimates that such abuse may cost from $3 to $5 billion per year (Gerboth, Hoenecke, and Briganti, 1989).[a]

[a] Some law enforcement officials estimate that the costs may be even higher (Steven Purdy, 1991, personal communication).

Besides blatant criminal acts, the widespread use of computers and related technology can lead to other forms of abuse as well. In particular, civil libertarians worry about the increasing use of information technology to invade people's privacy. In an era when stores use computers to collect personal data about their customers, on-line services track the information each consumer accesses, and credit bureaus compile detailed financial data on individuals (Gandy, Summer 1989), questions arise about who should control and have access to all this personal information. Striking a balance between the desire to exploit information technology for economic gain and the need to protect personal privacy requires an informed citizenry.

What values will today's children and tomorrow's adults apply when taking advantage of computers and other information technology? Our educational system bears a major responsibility for helping to shape these values.

## HOW TECHNOLOGY CAN AFFECT ETHICAL AND UNETHICAL BEHAVIOR

Why, you might ask, is it necessary to treat ethical behavior related to the use of information technology any differently than ethical behavior in general? If families, schools, and other social institutions are successful at passing on to children our society's traditional notions of right and wrong, won't they apply them to the use of information technology as well? Not necessarily.

While many of our traditional values can be stretched to fit the new environment of information technology (Johnson, 1990), some aspects of this new environment can make the fit difficult for people to see. A child who would never think of searching through a classmate's desk to read her personal diary might feel free to access and read the same classmate's diary stored in a word processing file on a network. A teenager who would never dream of robbing a bank, might experience fewer qualms about attempting to steal funds from the bank electronically. Why?

One explanation is that technology removes us from the concrete object: the book, the actual money. Another explanation is that, by using the computer to commit an unethical act, the perpetrator often believes that he or she can escape detection. As the fear of being caught decreases, so does the student's need to engage in soul-searching.

Information technology also introduces *psychological distance* to the scenario (Friedman, April 1990a). When we interact with others face-to-face and behave unethically, we experience first-hand the harm we have caused—and the resulting feeling can reinforce our ethical norms. When we use information technology in a way that does harm to others, the act feels less personal because we can't see or hear the other person in the exchange. We may not experience him or her as a person at all (DeMaio, 1990, 1991). For instance, if a group of students gains unauthorized access to a corporate computer network, they might feel pleased that they have succeeded in "beating the system" but might never realize the disruption they have caused to the employees who run and use the network. The fact that information technology makes it easier to target victims we don't know and who don't know us, adds to the feeling of anonymity and distance.

## CONFUSION OVER INTELLECTUAL PROPERTY

Another challenge we face when teaching about the responsible use of technology is that we are forced to confront some complex and often confusing issues. While students and educators may have a firm sense of right and wrong when it comes to physical property, the use of computers and related technology more often concerns an intangible kind of property—information as property. And we are confused about how to regard information. Is it the free-flowing life blood of a naturally curious human society—something to be shared? Or is information the private property of its creators (DeMaio, 1990, 1991)? This conflict in the way we view information can be observed regularly in classrooms. On Tuesday, a small group of students might be encouraged to share their ideas in a computer-based, collaborative writing project. On Wednesday, one of these students might be reprimanded for not working independently on an individual writing assignment. Such mixed messages about information as involving both shared and private experience are a potential source of confusion for students, if not directly addressed in the classroom.

The use of information technology to both generate and disseminate information electronically further complicates matters. Computers and related technologies make it easy to write collaboratively (even at multiple locations), compile information from a variety of sources, copy it, revise it, and destroy earlier versions. As a result, it is often difficult to determine who the author is and who should have ownership rights to the information (DeMaio, 1990). And when ownership is unclear, the ethical imperative to respect the owner's property rights is considerably weakened.

Even if we agree about who has legitimate ownership rights to information, theft of electronically-stored information may seem less of an evil than theft of tangible property. If we steal a car, the victim is deprived of its use. However, if we steal information from a computer network, the victim usually still has access to the information and may never even realize that a theft has been committed. The perpetrator may believe that he or she hasn't harmed anyone.

Another area of confusion concerns the rights we gain when we purchase software. When we buy physical property (e.g., a bicycle, clothing), we gain the right to do virtually anything we want with it. However, in the world of intellectual property, our rights are not nearly as broad. For example, unless we have express permission from the software publisher, our rights do not extend to unlimited duplication (Johnson, 1991).

As we attempt to make sense of these complex issues, we cannot always trust our intuition about what is ethical and legal. We cannot assume that students will take the ethical high road--or always know which is the high road. Nor can we count on parents to provide ethical guidance in the realm of information technology. Often, parents do not have sufficient experience with information technology in their daily lives to fully understand the ethical and legal issues involved. It is up to the schools to become informed about the relevant legal and ethical issues and to provide the guidance students need.

# WHAT SCHOOLS CAN DO

Schools have a major role to play in reinforcing traditional societal values and helping students see how these values apply to the use of information technology. Schools can also help prepare students to maneuver intelligently through the uncharted ethical waters they are bound to encounter in the world of technology.

Schools can take action on technology ethics on two fronts: setting school policy that provides a model for students to follow, and incorporating technology ethics issues into the curriculum.

## Defining and Implementing School Policy

The only way to ensure that the school and its personnel serve as models in the ethical use of information technology is to establish clear, implementable policies regarding such use. In setting these policies, decision-makers need to know how technology is being used in the district and anticipate how it will be used in the near future. Are local area networks in place? Are students and teachers planning to become involved in telecommunications projects with other sites (within or outside the district)? Do schools in the district have (or plan to buy) equipment that makes it possible to capture images, sounds and computerized material and incorporate them into multimedia presentations? For each anticipated use, it is necessary to be aware of the specific challenges and ethical dilemmas that might arise, and to become informed about the relevant legal issues. (See Box 2 for more about laws and legal issues.)

## Box 2

## Information Technology and the Law

Federal Copyright Protection for Computer Programs. A 1980 amendment[a] to the 1976 Copyright Act gives computer programs the same basic protection as other original works of authorship. The law allows the creation of a copy for archival (backup) purposes only. If one loads the program onto a hard drive, one may keep the original for backup (U.S. Congress, Office of Technology Assessment, April 1986). There is some debate over whether *multiple-loading*, or using the same disk version of a program to load it in several computers at once, violates copyright law (International Society for Technology in Education, March 1987). Some experts believe it is a violation because multiple-loading actually creates many temporary copies of the program.

Software License Agreements. Under software licensing agreements, schools do not technically purchase software but rather purchase the rights to use it in the manner specified in the agreement. In the case of a site or network license, schools are granted the right to duplicate or widely distribute the product. (See Box 3 for more information about such licenses.) In addition, many educational software publishers now include a software agreement with every *individual* software package they sell. With some products, the school indicates its consent to the agreement by tearing open the clear plastic shrink-wrapping. In other cases, an authorized school official indicates consent by signing the warranty card. When some form of consent is required and given, software licensing agreements are generally assumed to be legally binding. Some states have passed laws making the terms of such agreements enforceable (Reed, July 1989).

Fair Use. The 1976 Copyright Act provides for *fair use* exceptions[b] to the otherwise exclusive rights of copyright holders to "*distribute*, *perform*, or *display* copyrighted works (U.S. Congress, Office of Technology Assessment, April 1986)." The term fair use is not defined in the statute but is generally interpreted to include reproduction. Four factors are considered when determining whether a use is fair:

1. The purpose of the use (non-profit educational purposes are usually considered acceptable)
2. The nature of the copyrighted work
3. The amount and proportion of the whole copyrighted work used (the smaller the proportion, the more likely the use will be considered fair)
4. The effect the use might have on the copyrighted work's market potential or value (U.S. Congress, Office of Technology Assessment, April 1986)

The interpretation of these factors has been left to the courts. It is difficult to predict how they will be applied to educational uses of electronically-stored databases and library collections of graphics and sounds.

Unauthorized Access as Computer Crime. The Credit Card Fraud Act of 1984[c] prohibits the fraudulent use of any card, plate, code, account number, or other means of account access that can be used alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds. The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984[d] prohibits unauthorized access to computer systems run or used by the federal government or financial institutions, as well as systems run by credit card companies and consumer reporting agencies (Purdy, 1990). Most states have laws that specifically prohibit unauthorized access to computers (McEwen, June 1989).

Legal Liability For School Computer Networks. Based on a review of relevant law, judicial rulings, and legal opinion, researcher Early Dowdy (August 1989) warns that a school district or its employees may be liable for personal injury or property damage caused by student actions or communications involving a district-run computer network. Liability will vary from state to state and may hinge on the adequacy of supervision. If students distribute defamatory statements over a network, they could be considered publishers under libel law, and the school district could be considered a republisher. The 1988 Supreme Court ruling in *Hazelwood School District* v. *Kuhlmeier*[e] gave public school districts the power to control the content of publications sponsored by districts. Regarding computer networks, districts may have the corresponding legal responsibility to wield this power, in the form of monitoring (Dowdy, August 1989).

[a] See 17 United States Code (U.S.C.) Secs. 101 and 117.
[b] See 17 U.S.C. Sec. 107.
[c] See 18 U.S.C. Sec. 1029.
[d] See 18 U.S.C. Sec. 1030.
[e] See 484 U.S. 260 (1988).

Effective implementation of whatever policy is decided upon relies in large part on teachers. It is not possible to enforce new rules or have a positive effect on the attitudes of students without support from the classroom teachers in the district. Ideally, the teachers most involved in technology use should, from the start, play an active role in formulating policy—helping to define the problem areas and arrive at realistic solutions. Once policy is set, it is crucial that it be communicated to all faculty and staff members. One effective way of doing so is to give the discussion of district policies on ethics and the law a high priority when planning technology-related staff development activities.

Unauthorized Software Copying. Regardless of how computers are used in the school, unauthorized copying of software will remain tempting to some teachers and students, and needs to be addressed via policy. Since the legal and ethical issues are similar, districts may want to relate their software copying policy to policies on videotaping and photocopying. In addition, there are some useful resources that can help educators focus on the specific legal issues related to software use and duplication.

One such resource is a policy statement on software copyright issued by the International Council for Computers in Education (ICCE) in 1987.[8] Another is a single-page handout, released by the Software Publisher Association (SPA) in 1991, that answers questions about software copying from the industry's viewpoint.[9] Both resources address such issues as the creation of back-up copies and the use of local area networks. In addition, the ICCE statement offers a model district software copyright policy and some helpful hints for schools when setting guidelines. For example, recognizing that most software programs come with a license agreement that may place more specific restrictions on use than copyright law provides, the policy recommends that

> . . . *only* one person in the district be given authority to sign software licensing agreements. This implies that such a person should become familiar with licensing and purchasing rights of all copyrighted materials (International Society for Technology in Education, 1987).

Other steps for avoiding copyright infringement include providing secure storage for software, keeping up-to-date, centralized records of all software that has been legitimately purchased, and conducting periodic "audits" to make sure that the school is using only software that appears on those records (Gamble and Anderson, September 1989).

The SPA offers a free Self-Audit Kit to any institution that requests one. Although the kit is designed for businesses, it could be helpful to you if your school uses utility software (e.g., word processing and spreadsheet programs) on computers with hard disk drives. In addition to outlining steps for completing a self-audit, the kit includes a software program that searches the hard drive for many of the software applications used most often by business and generates a printed list, ready for comparison with the district's records of software ownership.

If your school distributes software throughout a local area network, your software license agreements must allow for network use. In addition, if the computer workstations attached to the network are equipped with floppy disk drives, the network software should be set up so that users cannot copy commercial software programs onto floppy disks.

Perhaps most important of all, policy-makers should make sure that faculty and students understand that unauthorized software copying represents theft of someone else's ideas and efforts. Faculty and students need to know what they can and cannot do under copyright law and under specific publisher's license agreements, as well as the ethical rationale for the law and license agreements–that software programs are the software developers' and publishers' intellectual property and that if users copy software rather than purchase it, the software developers' incentive to improve products over time and to develop new, better quality products is reduced. Faculty and students should also know in advance the penalties they face for violating the policy. For instance, one district policy states that "legal or insurance protection . . . will not be extended to employees who violate copyright laws."[10] And some technology companies go so far as to make unauthorized software copying by their employees an offense punishable by dismissal.

It is also important to anticipate the consequences of a policy against unauthorized copying and to consider how it relates to other decisions about educational technology. One recent study suggests that if teachers face the choice between unauthorized copying and insufficient software resources for their students, some teachers will choose to copy (Friedman, April 1990b). To address the problem realistically, therefore, districts need to offer teachers reasonable alternatives. Although eliminating illegal copying may result in a decrease in the amount of software available in some schools, a district can help ensure broad access to quality programs by actively pursuing legal and affordable purchasing options.[11] (For more information on purchasing options, see Box 3.) In addition, a number of schools and districts have come up with innovative approaches to fund-raising (e.g., students teaching after-school technology courses to the community; selling videocassettes of school sports events) to supplement the existing technology budget.

## Box 3

## Cost-Effective Purchasing Options for Schools

Lab Packs. Most educational software publishers offer this option to schools interested in buying multiple copies of a program for use in a single computer lab or classroom. A lab pack generally consists of several copies of the program (five-packs and ten-packs are common) accompanied by a single set of documentation. The entire lab pack costs considerably less than purchasing an equivalent number of individual software packages.

Site Licenses. This is a cost-effective approach to acquiring programs that are to be widely used throughout a school or district. In granting a site license, a publisher generally gives the licensee the right to make unlimited copies of the program for use within a specific "site." The site might be an individual school building, a district, or any other unit that the two parties agree upon. Some companies have a standard rate they charge for a certain type of site license; others base the price on the number of potential users at the site.

Network Licenses. Since distribution of software via a local area network can be seen as a form of duplication (because the software is available at more than one computer workstation at a time), most networkable versions of programs come with a license that determines how the software is to be used on the network. Some licenses allow for unlimited use of the program on a single local area network. Others define the number of network users (or workstations) that can have access to the program at any one time. (Such limits are then enforced by the network management system which alerts users who attempt to access certain programs that all available copies are currently in use.) Pricing varies but tends to be much more cost-effective than the purchase of the equivalent number of individual copies intended for stand-alone (non-network) use.

Other Volume Discounts. In addition to lab packs and licenses, most educational software companies offer other discounts to institutions and groups that make large purchases. Some companies deduct a percentage of the cost for each order over a certain size; others offer "district memberships" that provide price breaks to participants ordering many products over a longer period of time. Some larger entities--occasionally including entire states--have been able to negotiate special price breaks from software companies by placing especially large orders, or even by helping with the development of new products. Although individual schools and districts do not have the same buying power as a large state, a number of them have found ways of saving money by grouping together to place bulk orders. Most educational software companies are receptive to proposals for affordable ways of making large purchases (Salpeter, January 1988).

Software Bundling. Many educational software companies offer special discount pricing for "bundles" of software that include several related titles or a number of programs in a series. Increasingly, we are seeing partnerships between different companies (often including both hardware and software providers) to deliver cost-effective bundles addressing specific needs (e.g., teacher productivity, elementary language arts).

Fair Use.[12] As multimedia becomes a regular part of the instructional process, many teachers have questions about the legality of incorporating commercially-available information, including downloadable text from CD-ROM databases, graphics libraries available on floppy disks, and digitized music recordings, into computer-based presentations that they and their students create. While the *fair use* exceptions to copyright law can be interpreted as giving educators limited rights to capture such materials for educational purposes (essentially, *duplicating* the source material by incorporating it into a new presentation), current law is not definitive about these issues. One logical policy solution is to seek written permission from the publisher whenever information is to be used in a project that will be distributed beyond the classroom.

Plagiarism and Giving Credit. Schools will probably want to extend existing rules against plagiarism to include all forms of electronically-stored information. Setting district-wide standards for giving credit to all information creators (e.g., authors, graphics artists, publishers) when excerpting electronically-stored information is a good way to guard against even unintended plagiarism. For example, if a student develops a multimedia project that incorporates graphics from a graphics library disk and text from a CD-ROM encyclopedia and an online database, he or she should be expected to cite all of these sources in a bibliography that accompanies the project.

Electronically-Stored Information As Property. When information is stored in electronic form, it is subject to the same ethical standards as print-based information and tangible property. Many school districts have policies in place regarding issues such as theft and vandalism. They need to articulate how these policies should apply to technological versions of such wrongdoing. For example, if vandalizing school walls is a suspendable offense, will the same action be taken if a student deliberately tampers with a file on the school's network? If technology-based theft or vandalism seems less serious than the old-fashioned kind, consider the damage that can be done when students use computers, modems, and telephone lines to connect to district-wide, nationwide, or even worldwide networks.

Confidentiality and Privacy. Computer security expert Harry B. DeMaio (1991) notes that an effective program designed to reinforce respect for confidentiality and privacy must go beyond a general "statement of policy and an occasional awareness meeting." He stresses that the program must address the specific needs of the target organization. School districts can apply DeMaio's advice by identifying the different types of files that require a high degree of confidentiality, determining who should have access to each type of file and why, and then setting up a system for restricting unauthorized access.

One area of particular concern for schools is the amount of sensitive personal data (e.g., the results of psychological testing, financial information about students' families, etc.) that a district must store. The responsible care of confidential information is an important legal and ethical issue for our society as a whole. As more and more data become stored on interconnected computer networks, passwords and access codes are replacing locked doors and file cabinets. A school administrator who would never leave sensitive data in an unsupervised, unlocked file cabinet might not think to set up adequate password protection for the same data on a computer-based system. One major manufacturer of computers and school networking software recommends at least three levels of password protection when using networks with students in grade four and above–one level for students, one for teachers, and one for administrators and system managers. Larger districts may need even more levels of protection.

When dealing with student-created files, schools are faced with a different challenge: how to balance respect for an individual's privacy with the responsibility for monitoring student academic performance. Some school districts may choose to guide this balancing act via policy. For example, they may want to define certain writing (e.g., journals) to be private–off limits to teachers without student permission. Whatever policy is set, it is important for students to be informed about who will have access to which of their files. As information technology advances, such privacy issues are likely to multiply. For example, when using a network system that allows teachers, from their teacher workstations, to observe students while they work, the school will want to set a policy of letting students know when they are being observed.

<u>Free Speech vs. School Responsibility</u>. Some schools have faced the challenge of balancing student free speech and the school's quasi-parental role in the context of student newspapers. Regional, national, and international computer-based school networks will place schools in the position of being electronic publishers–with a vastly larger potential audience than the local community. Some schools may want to specify in policy what the school's role will be in screening electronic publications for ethical abuses such as defamation and profanity.

Telecommunications Policy. The ethical issues that arise when students use computers to telecommunicate are not very different from those related to the use of stand-alone computers and local area networks. However, the impact of telecommunications abuse is more widespread (since it involves students at multiple sites) and the responsibility for monitoring user behavior often falls outside the local school. In establishing an effective policy in this area, decisionmakers must consider the purposes for which students will telecommunicate (e.g., use of an e-mail system for pen-pals; use of a bulletin board as a forum on controversial issues). They must also understand the standards, procedures, and monitoring policies of the online services that will be used.

School districts will want to ensure that students are aware of accepted standards of behavior on online systems (e.g., avoidance of defamatory or obscene remarks). Districts will also want to take a clear stand against the use of telecommunications to engage in software piracy or to violate others' right to privacy. In addition, schools and districts should aggressively discourage the illegal use of telephone and telecommunications systems–including telephone fraud, unauthorized use of such systems, and deliberate crashing of network-based computer systems. Finally, policies and procedures should be in place that will minimize the risk of computer viruses. Effective strategies include the use of anti-virus software, discouraging the use of outside or pirated software within the schools, and controlling access to the school's or district's own networks.[13]

## Incorporating Technology Ethics Issues Into the Curriculum

For technology ethics issues to have an impact on students, they need to be addressed in classrooms and computer labs as part of the instructional process. To encourage this, some districts have included technology ethics as a content strand in their formal curriculum guidelines. It is recommended that experienced, technology-using teachers be involved in the process of developing the technology ethics curriculum strand. Before the curriculum strand can be effectively implemented, the content and appropriate instructional methods need to be addressed as part of in-service, teacher education.

What to Teach. An overriding theme of technology ethics instruction is that information technology systems–including hardware, software, and data–are extensions of human society. They are created by humans and used by humans. They can be used to benefit others or to harm them. Some applications of information technology are ethical and others are unethical. Still other applications are in the ethical "gray zone." Each individual has a moral responsibility for how he or she uses technology.

Specific topics that school districts may want to address as part of a technology ethics curriculum include respect for privacy and confidentiality, respect for information technology systems as property, respect for intellectual property rights, conflicts between competing rights (e.g., freedom of information vs. privacy), and the law as it applies to the use of information technology.

When to Teach. Technology ethics issues can be infused into the curriculum at different grade levels. Some districts target technology ethics instruction at the middle school or junior high grades—at an age when many students develop sufficient computer expertise to cause significant damage. However, many experts in the field recommend beginning technology ethics instruction when students are first introduced to technology. A recent survey showed that more elementary students use computers in school than high school students (National Center for Education Statistics, 1991). Paul Resta of the University of Texas Learning Resource Center suggests a spiraling ethics curriculum—starting instruction in the elementary grades and continuing throughout the grade range at increasing levels of sophistication.[14]

Where in the Curriculum. Technology ethics have typically been introduced in subject areas with a heavy technology focus, such as computer literacy, computer programming, and vocational education. As schools move to incorporate technology throughout the curriculum, some believe that ethics must be addressed whenever students use technology. Others recommend including technology ethics as part of the social studies curriculum, science or math curriculum—so it will be assured of a permanent curriculum home.

Instructional Strategies and Activities. A variety of instructional strategies and activities have been tried, including assigned readings, computer-based activities, writing assignments, role-playing, and classroom discussions.

There are few published sources of information on technology ethics intended for students. One exception is a textbook recently published by South-Western Publishing, entitled *Telecommunications: Concepts & Applications* (Cubbler, Olivo, Jr., and Scrogan, 1991), which includes a section specifically focusing on ethics in telecommunications. Exsym, Inc. (1987) publishes *Ethics: Online*, a kit designed to help schools to teach telecommunications ethics. The kit includes a software demonstration disk for illustrating ethics topics during classroom discussion, a set of positive ethical guidelines, information on legal consequences of illegal online behavior, and a set of ethical issues cards that can be used to stimulate role-playing, group discussion, or student writing. Exsym also publishes *The Electronic Village* (1989) and *The Electronic Mailbag* (1990), which introduce electronic bulletin boards and e-mail systems, respectively. Both products cover ethical issues.

*The Computing Teacher*, ISTE's monthly journal, published articles in 1984 that discussed and provided examples of two valuable instructional techniques:[15] student role playing and classroom discussions based on scenarios that involve technology and present dilemmas with no easy solution.[16] The information in these articles can still be applied to technology ethics instruction today. For example, one role playing exercise involves a situation in which a student named Andy has purchased a popular computer game. A friend, who has given Andy copies of other games in the past, asks him for a copy. Other participants in the situation include a student whose mother developed the computer game and another student who is knowledgeable about copyright law. Groups of four students role play the situation and then report the results to the whole class.

Some districts have developed their own materials. For example, a San Antonio, Texas, district includes in its middle school computer literacy curriculum a passage on computer crime that ends with several ethical questions. The passage is presented as a word processing file with many words deliberately misspelled. Students first use the passage to practice spell-checking and then go on to answer the ethical questions (Paschal et al., undated).

To encourage the development and sharing of strategies for technology ethics instruction, the Computer Learning Foundation (CLF) organized a contest for teachers, entitled *Teaching Children to be Responsible Computer Users*, as part of Computer Learning Month 1990. (See Box 4 for some of the best teaching ideas submitted by contest participants.)

## Box 4

## Teaching Ideas from the Computer Learning Foundation's Responsible Computing Contest[a]

First Place Idea: Elementary School Level

Develop a series of teaching units based on the Computer Learning Foundation's *Code of Responsible Computing* (or a code your school or district creates). In each unit, begin by introducing key concepts, including definitions, relevant legal and historical information (e.g., the right to privacy as addressed in the Bill of Rights and interpreted by the Supreme Court), and examples of personal relevance to students (e.g., other students going through their desks or lockers; someone borrowing their belongings without permission; a fellow student copying their school work). Then have students complete activity sheets that ask thought-provoking questions, such as:

How would you feel if your rights were violated? What should the consequences be for violators?

Should all people's property be respected and protected? What about their ideas and information stored on a computer? Are there any exceptions?

Activity sheets can also engage students in classification activities, such as classifying places and information sources as public or private (e.g., student's desk, principal's office, hallway, library book, personal letter), and classifying actions as requiring or not requiring permission (e.g., reviewing a classmate's story on disk, reading a bulletin on a bulletin board). Use the worksheets as a basis for whole class discussion.

First Place Idea: Secondary School Level

Involve students in a mock trial of a case involving unethical use of technology. Start by introducing the case and relevant concepts, such as court procedures and U.S. beliefs in trial by jury and in the presumed innocence of the accused until proven guilty beyond a reasonable doubt. Then have students assume different roles–lawyers, judge, jury, witnesses, plaintiff, and defendant–with each student researching the issues and positions of their roles. To integrate writing practice into the activity, direct all students to take notes during the trial. Have the lawyers prepare and present opening and closing statements, and decide which witnesses to call. When the trial is completed, organize a debate of the case and related issues during the students' social studies class.

Other Winning Ideas

- Have students view the movie, *War Games*. Then have them rank the actions observed in the movie on a continuum from most harmful to least harmful. Also have students research and discuss news stories involving computer crime. Finally, hold a class discussion on the consequences of the computer crimes they identified–consequences for the victims and for the perpetrators.

- Review with the whole class different license agreements included in software packages. Discuss how these agreements relate to existing laws. Have students compare license policies of different companies.

- Develop a short musical presentation with raps, songs, and musical instruments to get students' attention while communicating the importance of responsible computing. One teacher had characters in a musical costumed in garbage bags with cardboard characters attached. The characters included "Computerbug," who deletes software and adds bugs to software programs; "Bender," who bends disks and snatches disks from the disk drive when the red/busy light on the disk drive is on; "Copycat," who copies everyone's disks and sends them to all of his friends; and "Snatcher," who takes information and ideas from other people's disks and from other computers with a modem over telephone lines and makes them his own. In each scenario, a talking computer monitor saves the day and explains to students why they want to keep these villains away from the computer.

- Relate the teaching of computer ethics to the theme of pirates and Captain Hook. Have students prepare stories that are to be shared with other students in the class. After students submit their stories, present the stories on the bulletin board under the author, Captain Hook. Have the class discuss how it feels to have someone else take credit for their work. Also discuss the consequences if a present-day Captain Hook stole another person's ideas or work.

- Have students list personal facts about their own lives and then discuss which facts they would be willing to share with people and organizations they don't know. Have them décide whether this information should be available for sale to others.

- Have students conduct surveys of other students' attitudes about computer ethics issues.

- Have students develop posters or billboards to communicate positive ethical messages and standards regarding technology use to other students in the school.

- Issue student *technology licenses* after students have been introduced to and can demonstrate an understanding of responsible use of technology. Require these licenses for students' use of the computer lab during class or study halls. Suspend licenses for violations of responsible computing, with the length of time dependent on the severity of the infraction.

- Invite speakers whose professions involve information technology for the school's career day, and ask them to address ethical issues in their presentations.

[a] The information for this box was provided by Sally Bowman, Executive Director, Computer Learning Foundation. The winning entry for the elementary school level competition was submitted by Donald Bullock, Knolls Elementary School, Simi Valley, CA. The winning entry for the secondary school level competition was submitted by Alleta Baltes, Arapahoe School District #38, Arapahoe, WY. Other contributing teachers included: David Heath, Friends School of Baltimore, Baltimore, MD; Jeanine DeLay, Greeenhills School, Ann Arbor, MI; Margaret Snyder, All

Saints Catholic, Pottsville, PA; Pamela Mitchell, Pleasant County Middle School, Belmont, WV; Suzy Bagley, Kaley Elementary School, Orlando, FL; Louise Kaan, Dildine Elementary School, Cheyenne, WY; and Robbi Ray, Bruce Middle School, Louisville, KY.

Another learning activity idea comes from CLF's *Storybook on Responsible Computing* competition for students.[17] Teachers prepared students for writing by introducing the CLF *Code of Responsible Computing*[18] and leading class discussions on the different legal and ethical issues addressed in the Code. Then the students were directed to create storybooks (fiction or non-fiction) with the theme of responsible computing. Storybooks included heroes and heroines championing positive computer ethics; student fables, each with a moral involving computer ethics; and serious essays on the importance of responsible computing.

Some advocates of technology ethics instruction recommend that students gain experience with the decisionmaking involved in running a computer network. They suggest that groups of students run a class-wide electronic bulletin board and e-mail system on a rotating basis–and have the responsibility for deciding what should and should not be done on the network. This opens up the possibility of confronting–in a controlled environment–many of the technology ethics issues that occur in the real world.

Educators who have used hypothetical scenarios in elementary through junior high school find that the best scenarios are ones that compare technology abuse with familiar situations to which traditional values can be applied or that make it easy for students to identify with the victims of abuse. For example, a teacher who wanted her class to explore the ethics of unauthorized software copying, had her students imagine that they were members of a rock band that had been writing songs and practicing for two years, and finally had a hit recording. The teacher asked her students to discuss how they would feel if someone bought their CD and made copies for everyone they knew–or if a lot of people started making copies. She then moved the discussion to software copying, providing enough background information about software publishing so that the students could draw the ethical analogy.[19] (See Box 5 for additional scenarios.)

## Box 5

### Scenarios to Stimulate Technology Ethics Classroom Discussion

Theft of Intellectual Property. A group of students develops a design for a new, exciting product (e.g., a toy). The plans are kept in one student's locker or are stored on a computer network. Someone breaks into the locker or network, steals the plans, and manufactures the toy.[a]

Invasion of Privacy. A boy and a girl like each other a lot and have been exchanging love poems, either by passing notes in the school lunch room or by sending each other messages on a network e-mail system. Another student gets hold of the notes from the students' desks or invades the e-mail system and reads the poems.

Destruction of Private Property. A student has been working on a school report, stored as a file on a computer network. When she accesses the file, she discovers that every fifth word is missing—someone has messed with her file! After school, she goes to unlock her bike from the bike rack and discovers that the pedals are missing.

[a] Carol Brummer, Canyon Middle School, New Braunsfel, TX, 1991, (personal communication).

At the high school level where students are capable of handling more complex issues, teachers may want students to explore emerging ethical dilemmas involving technology. Some issues to focus on might be

- the ability to combine information from different electronic data sources to develop data profiles on individuals or neighborhoods —usually for marketing purposes; permission for this use of the data is rarely sought or given

- the practice of some commercial computer network services to monitor and censor user communication on their electronic bulletin boards and e-mail systems

- the reliance on computer-based systems for important societal functions (e.g., air traffic control), despite the fact that such systems are subject to both human error and mechanical failure (Forester and Morrison, 1990)

- the possibility that government information may someday be available *only* in electronic form accessible via computer-based systems

- the possibility that laws against unauthorized access or use of electronically-stored data may prevent "whistle-blowers" from informing journalists about corporate or government wrongdoing

- the development of technology-based systems to replace human workers and the resulting problems related to job displacement

Issues such as these can be effectively introduced through scenarios. Deborah G. Johnson (1990), of the Department of Science and Technology Studies at Rennselaer Polytechnic Institute, recommends that scenarios should be presented in a context that includes extensive classroom discussion. She suggests that teachers should plan for such discussions by developing questions and discussion guidelines to accompany each scenario.

Informal Curriculum. Finally, it is important to remember that every classroom and computer lab has an informal technology ethics curriculum—the behavior of teachers whom students may emulate, and the rules for responsible technology use that students are required to follow. School policy—one that includes teacher education—can help ensure that teachers serve as models of legal and ethical behavior. Rules for ethical use of technology can become lifetime habits, especially if students understand and internalize the values behind the rules (Scrogan, February 1988).

## SUMMARY

As the use of information technology continues to rise—both in our schools and throughout our society—the need to address the ethics of technology use grows. The potential for criminal abuse is on the rise, and some applications of technology challenge our nation's core values (e.g., the right to privacy; the right to free expression).

It is not new for our educational system to teach about ethics, but as the use of educational technology increases, so does the complexity of the task faced by educators. Although many of our traditional societal values can be extended to the use of information technology, the nature of this technology (e.g., the *psychological distance* it creates) may make it more likely that, without educational intervention, some individuals will act unethically. Adding to the challenge is many people's confusion about intellectual property rights, especially as they apply to information that is stored and disseminated electronically.

Schools have a vital role to play in helping our children understand how existing values, policies, and laws apply to a rapidly changing, information technology-dependent world. To be effective in this role, educational policymakers must understand the ethical dilemmas and legal issues raised by each of the information technologies in use in schools. They must set realistic policies that comply with the law and that model ethical behavior for all involved. And they must educate teachers about important technology ethics issues and must clearly communicate related school policies to both faculty and students. Equally important, by incorporating the study of technology ethics into the standard curriculum, schools can ensure that the leaders and decisionmakers of tomorrow will be equipped to make the difficult ethical decisions they will undoubtedly face.

# Endnotes

1 Sending *electronic mail* is the computer equivalent to sending a personal letter. It typically involves only two parties and is usually intended as private rather than public communication.

2 Communication via an *electronic bulletin board* typically involves more than two participants. Use of a bulletin board is usually thought of as a form of public communication.

3 A *virus* is a self-replicating program that causes erasures or alterations to computer programs or data files—usually ones stored on hard disks. Since a virus can copy itself onto other programs and onto floppy disks, it can travel from computer to computer, each time *infecting* the new machine (Forester and Morrison, 1990).

4 *Telecommunications*, as used here, refers to the use of a computer, connected to a device called a *modem*, to communicate with other computer-users or to access centralized databases over standard telephone lines. Students typically communicate via an online service that coordinates the activities of its users. Online services are run by for-profit companies, non-profit organizations, and sometimes by school districts themselves.

5 *Intellectual property rights* are the legal rights granted to authors, artists, inventors, and other "creators" (and sometimes their employers) to control the use and dissemination of their original ideas or their unique ways of expressing ideas (U.S. Congress, Office of Technology Assessment, April 1986). For a further discussion of intellectual property, see the section of this paper, Confusion Over Intellectual Property, beginning on page 6.

6 Richard C. Hollinger, 1991 (personal communication).

7 Transfer Agreement between the Department of Education and the National Institute of Justice, 1990 (unpublished document).

8 In 1989, ICCE became part of the International Society for Technology in Education (ISTE). The ICCE policy statement is available free of charge from ISTE, located at 1787 Agate Street, Eugene, OR 97403-1923.

9 The handout, titled *Is it okay for schools to copy software?*, is available free of charge from the SPA, located at 1730 M Street NW, Washington, DC 20036.

[10] *Comal Independent School District: Policy on Software Copyright,* New Braunsfel, TX: Comal Independent School District.

[11] Such an approach can help schools ensure that all students, regardless of ability or disability, have equal access to a variety of valuable technology-based learning experiences. While the equitable distribution of educational technology is not the focus of this paper, it is an important ethical issue that our society must address.

[12] For an explanation of the term, *fair use*, see Box 2: Information Technology and the Law, on pages 8-9.

[13] Len Scrogan, 1991 (personal communication).

[14] Paul Resta, 1991 (personal communication).

[15] The articles from the August/September 1984 edition of *The Computing Teacher* are "Ethics and Computer Use" by Kay Gilliland and Mattye Pollard, and "A Question of Ethics" by Larry S. Hannah and Charles B. Matus. Each is available from ISTE for a $1 handling fee. (See footnote 8 for ISTE's address.)

[16] The first known use of scenarios in technology ethics education was by Donn Parker (1979) *Ethical conflicts in computer science and technology.* Menlo Park, CA: SRI International.

[17] The information about this CLF contest was provided by Sally Bowman, Executive Director, Computer Learning Foundation.

[18] The Computer Learning Foundation's *Code of Responsible Computing* provides guidelines for ethical use of technology. The Foundation can be contacted at P.O. Box 60007, Palo Alto, CA 94306-0007.

[19] Carol Brummer, Canyon Middle School, New Braunsfel, TX (personal communication).

# REFERENCES

Cerow, W.P. (1989) *Unethical & illegal computing practices: Parent and teacher awareness presentation.* Wayne P. Cerow, Cerow Investigations & Consultants, Inc.

Cerow, W.P. (1989) *Unethical & illegal computing practices: Student awareness presentation.* Wayne P. Cerow, Cerow Investigations & Consultants, Inc.

Computer Learning Foundation (1990-1991) Code of responsible computing. *Computer Learning Month*, p 10.

Conly, C.H. (July 1989) Organizing for computer crime investigation and prosecution. *National Institute of Justice: Issues and Practices.* Washington, DC: U.S. Department of Justice, Office of Justice programs, National Institute of Justice.

Conly, C.H and McEwen, J.T. (January/Febrary, 1990) Computer Crime. *NIJ Reports, A Bimonthly Journal of the National Institute of Justice*, No. 218., pp. 2-7.

Cubbler, C.D., Olivo, J.J., Jr., and Scrogan, L. (1991) *Telecommunications: Concepts & applications.* Cincinnati, OH: South-Western Publishing Co.

DeMaio, H.B. (1991) Information ethics–it doesn't come naturally. *Computer Security Journal*, Vol. V, No. 1.

DeMaio, H.B. (1990) Information ethics, a private perspective. Invited paper presented to the National Institute of Justice, Professional Conference on Information Technology Ethics, April 27-28, Washington, DC.

Dowdy, E. (August 1989) School computer networks: Electronic publishing and legal liability in the public school. Paper presented at the Annual Meeting of the Association for Education in Journalism and Mass Communication in Washington, DC.

Exsym, Inc. (1990) *The electronic mailbag.* Portland, OR: Exsym, Inc.

Exsym, Inc. (1989) *The electronic village.* Portland, OR: Exsym, Inc.

Exsym, Inc. (1987) *Ethics: Online*. Portland, OR: Exsym, Inc.

Forester, T. and Morrison, P. (1990) *Computer ethics*. Cambridge, MA: The MIT Press.

Friedman, B. (April 1990a) Moral responsibility and computer technology. Paper presented at the Annual Meeting of the American Educational Research Association in Boston, MA.

Friedman, B. (April 1990b) Societal issues and school practices: An ethnographic investigation of the social context of school computer use. Paper presented at the Annual Meeting of the American Educational Research Association in Boston, MA.

Gamble, L.R. and Anderson, L.S. (September 1989) Nine easy steps to avoid software copyright infringement. *NASSP Bulletin*, pp. 90-93.

Gandy, O.H., Jr. (Summer 1989) The surveillance society: Information technology and bureaucratic social control. *Journal of Communication*, Vol. 39, No. 3, pp. 61-76.

Gerboth, D.L., Hoenecke, J.B., and Briganti, R. (1989) *White collar crime: Loss prevention through internal control*. New York: Ernst & Young (prepared for the Chubb Group of Insurance Companies).

Gilliland, K. and Pollard, M. (August/September 1984) Ethics and computer use. *The Computing Teacher*, pp. 19-23.

Hannah, L.S. and Matus, C.B. (August/September 1984) A question of ethics. *The Computing Teacher*, pp. 11-14.

Herig, J.A. (1989) *Computer crime in Florida*: 1989. Tallahassee, FL: Florida Department of Law Enforcement.

Hollinger, R.C. (1990) Ethics, crime, and the computer revolution: A sociological overview. Invited paper presented to the National Institute of Justice, Professional Conference on Information Technology Ethics, April 27-28, Washington, DC.

Hollinger, R.C. (1989) Statistics on computer crime: A review of the research questions. Invited paper presented to the National Institute of Justice, Professional Conference on Computer Crime, September 14-15, Washington, DC.

International Council for Computers in Education (February 1987) Code of ethical conduct for computer-using educators: An ICCE policy statement. *The Computing Teacher*, pp. 51-53.

International Society for Technology in Education (March 1987) 1987 statement on software copyright: An ICCE policy statement. *The Computer Teacher*, pp. 52-53.

Johnson, D.G. (1991) Computers and ethics. In L. Becker (ed.) *The Encyclopedia of Ethics*. Garlund.

Johnson, D.G. (1990) A framework for thinking about computer ethics. (Unpublished paper.)

Martin, L.G. (1990) Unethical "computer" behavior: Who is responsible? Invited paper presented to the National Institute of Justice, Professional Conference on Information Technology Ethics, April 27-28, Washington, DC.

McEwen, J.T. (December 1990) Computer ethics. (Unpublished e-mail document.)

McEwen, J.T. (June 1989) Dedicated computer crime units. *National Institute of Justice: Issues and Practices.* Washington, DC: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice.

National Center for Education Statistics. (1991) *The Condition of Education,* Vol. 1, pp. 56-57.

Parker, D. (1979) *Ethical conflicts in computer science and technology.* Menlo Park, CA: .SRI International.

Paschal, L. et al. (undated) *Computer Literacy Curriculum Guide.* San Antonio, TX: North East Independent School District.

Purdy, S. (1990) Computer ethics: A law enforcement perspective. Invited paper presented to the National Institute of Justice, Professional Conference on Information Technology Ethics, April 27-28, Washington, DC.

Reed, M.H. (July 1989) *Computer software: Copyright and licensing considerations for schools and libraries.* Syracuse, NY: ERIC Clearinghouse on Information Resources (ED308856).

Resta, P. (1990) Computer ethics and students: The educational challenge. Invited paper presented to the National Institute of Justice, Professional Conference on Information Technology Ethics, April 27-28, Washington, DC.

Rosenblatt, K. (1990) In defense of privacy: A law enforcement perspective on the nature of computer intruders and how to deter them. Invited paper presented to the National Institute of Justice, Professional Conference on Information Technology Ethics, April 27-28, Washington, DC.

Salpeter, J. (January, 1988) Have it your way; how publishers respond to your needs, Classroom *Computer Learning* (now *Technology & Learning*), pp. 34-43.

Scrogan, L. (February, 1988) The online underworld. *Classroom Computer Learning* (now *Technology & Learning*), pp. 58, 60.

Software Publishers Association (1991) *Is it okay for schools to copy software?* Washington, DC: Software Publishers Association.

Thomas, J. and Meyer, G. (1990) In defense of the computer underground: Interpreting a cyber-culture. (Unpublished paper.)

U.S. Congress, Office of Technology Assessment (March 1990) *Computer software and intellectual property-Background paper,* OTA-BP-CIT-61. Washington, DC: U.S. Government Printing Office.

U.S. Congress, Office of Technology Assessment (April 1986) *Intellectual property rights in an age of electronics and information,* OTA-CIT-302. Washington, DC: U.S. Government Printing Office.

# Appendix

## List of Associations and Agencies to Contact for Further Information

Association for Computing
Machinery
11 W. 42nd Street 3rd Fl.
New York, NY 10036
212-869-7440

Association for Educational
Communication and Technology
Suite 820
1025 Vermont Avenue, N.W.
Washington, DC 20005
202-347-7834

Computer Learning Foundation
2165 Park Boulevard
Palo Alto, CA 94306
415-327-3347

Data Processing Management
Association
505 Busse Highway
Park Ridge, IL 60068
708-825-8124

Division of Technology
Development
Texas Education Agency
Contact: Connie Stout
1701 North Congress Ave.
Austin, TX 78701
512-463-9091

International Society for
Technology in Education
1787 Agate Street
Eugene, OR 97403-1923
503-346-4414

Institute for Certification
of Computer Professionals
Suite 268
220 E. Devon Avenue
Des Plaines, IL 60018
708-299-4227

Institute of Electrical and
Electronic Engineers
345 E. 47th Street
New York, NY 10017
212-705-7900

National School Board
Association
1680 Duke Street
Alexandria, VA 22314
703-838-6770

Software Publisher Association
Suite 700
1730 M Street, N.W.
Washington, DC 20036
202-452-1600

**U.S. Department of Justice**
Office of Justice Programs
*National Institute of Justice*

*Washington, D.C. 20531*

Official Business
Penalty for Private Use $300