CHAPTER 5

Social, Ethical, Legal, and Human Issues

- How does technology use contribute to social and equity issues in schools?
- What are the ethical issues presented by technology in education?
- In what ways can computer users avoid computer viruses, spam, email scams, and phishing?
- In what ways can education overcome the ethical, equity, and social concerns about technology in the schools?
- What effect does cybercrime have on education?
- How safe are the social networking sites for students?
- How is social networking affecting education?
- How can teachers use social networking in the classroom?
- What is the status of the digital divide?
- List several approaches to ensure privacy, protect assets, confirm identity, and guard against unauthorized access.
- What steps would you take to ensure child safety on the WWW?
- What are the implications of cyber safety for a teacher?
- Give examples of activities which violate the copyright law.
- What are the most common classroom copyright infractions?
- How can you make students aware of copyright law?

Computers are now so pervasive in our society that the question of how they can be used most wisely, efficiently, and ethically is a human issue that demands the attention of anyone interested in computer use. Although many of the purposes for which computers are used are extremely beneficial to the individual and to society, there is a wide range of misuse as well. For the past several decades, science fiction writers, philosophers, educators, and many others have been warning us about dramatic changes that computers will cause in our lives. What will these changes be? How will we adapt to such drastic reorganization of our routines? Implementation of these changes and adaptations requires that we act responsibly with our new technologies. How do we, as pioneers and educators, encourage ethical behavior on the technological frontier? We must grapple with these issues now if we are to shape a productive and humane future.
I CYBERCRIME

Cybercrime describes criminal activity in which computers, the Internet, or networks are a tool, computation device, or a place of criminal or illicit activity. Vamosi (2005) states that today, criminals are making more money from cybercrime than drug-related crime. Computer fraud, invasion of individual privacy, and freedom of speech are issues affecting our lives. The FBI reported (Evers, 2006) that dealing with viruses, spyware, PC theft, and other computer-related crimes costs U.S. businesses a staggering $67.2 billion a year (see Figure 5.1). In addition, the U.S. Secret Service reported telecommunication fraud losses are about $1 billion a year (Evers, 2005). This chapter will examine the contemporary social and human issues of computer crimes, security, and privacy, and the ethical, legal, and equity concerns in education.

I COMPUTER FRAUD AND MISUSE

Hundreds of thousands of large mainframe computers are used in the United States. People involved with these systems number in the millions. Many others have access to mainframes through personal computers. These figures add up to an alarming increase in incidents of computer abuse, especially computer-related crime, a trend that will likely continue into the future.

There are a variety of ways in which computers can be used to defraud others in our society. Theft of money can occur through criminal programming or intentionally inaccurate accounting transactions and rounded amounts. Stealing information from a computer and using a computer to market stolen information illegally are not uncommon practices. Many private companies and government agencies maintain computerized lists of their customers and clients. Once unauthorized personnel access these lists, the information can be sold to others for various uses. Theft of information is a serious concern to school personnel who store student records on computers. With access to a computer and the determination to break into confidential records, students have been known to alter the grades of their friends and enemies. The theft of computer time is another computer-related crime that is on the increase. People who

FIGURE 5.1 | FBI computer security survey.

Under attack
Almost a fifth of U.S. businesses said they suffered 20 or more incidents such as virus infections in an FBI survey of computer security incidents at companies in the past year.

1-4: 51.5%
20 or more: 19.2%
10-19: 20.1%
5-9: 9.1%

invade computer systems without authorization are called hackers, and their escapades are not always innocent.

Software piracy, or bootlegging, is the theft of computer programs. Software piracy occurs whenever a person purchases a computer program and then copies it for friends or resale. This is a violation of state and federal law, and those engaged in the practice are criminals. Software theft occurs on such a large scale that it costs an estimated $2.5 million each month—$1.0 million in actual losses and $1.5 million in lost sales opportunities. It is easy to copy computer programs, and for that reason, the victimless practice may appear harmless and practical. Unfortunately, piracy also occurs in the classroom. Many teachers are caught in a bind: They have a class full of students who want to use the same software at the same time, but there is not enough software to go around. Given the ease with which software can be pirated, it is tempting to make unauthorized copies. Although the act of piracy takes only a few minutes, the ramifications are long term. First, piracy sets a poor example for students, who are, after all, the computer users of the future. Second, it ultimately results in higher software prices because publishers must raise prices to compensate for losses through piracy. See www.spa.org for copying guidelines and other policies on software use. Piracy results in fewer legitimate customers and, consequently, higher-priced software packages.

Theft of identity is the fastest-growing white-collar crime. Victims’ identities are assumed through stolen Social Security numbers, drivers’ licenses, ATM cards, credit card information, and employee data theft. While impersonating their victims, criminals quickly spend as much money as possible before moving on to another stolen identity. Thieves can also use computer databases and the Internet to access large amounts of personal data. They steal passwords, Social Security numbers, and banking information from websites and employer databases. With this information, identity thieves apply for loans and make purchases over the Internet. Sometimes thieves “spam” or send unsolicited email offers requesting identification data. Naive email recipients provide the requested information, unaware of the fraud. Identity thieves create websites with links to legitimate sites to acquire passwords and credit card numbers. Some websites display forms and run scripts that provide unscrupulous webmasters with any information a person is foolish enough to post on an online form. Other information is mined directly from website visitors’ computers while they browse a site. Workers with access to company data can also steal employee and customer information either to use themselves or sell to others for fraudulent purposes. Today the Social Security and drivers’ license numbers of others, as well as business credit reports, individual credit reports, criminal records, civil records, bankruptcies, license verifications, marriage licenses, divorce records, death records, driving records, property records, utility records, and Social Security number verifications can all be accessed online (see www.infoseekers.com and www.fastbreakbail.com). Self-policing by the information broker industry has not restricted the sale of sensitive personal information to the general public. Evers (2005) reported that the overall cost to Americans of identity fraud reached $52.6 billion in 2004 and that, on average,
Social, Ethical, Legal, and Human Issues

victims of identity theft believe it took an average of 175 hours to remedy the theft of their identities, with average out-of-pocket expenses of $808 per victim (Benner, Givens, & Mierzwinski, 2000). New forms of secure technologies should minimize the risks of identity theft (see Maintaining Security in this chapter).

Malware: Computer Viruses, Spyware, Spam, Email Scams, and Phishing

Malware is any software which is created to attack, infect, or damage a computer system without the owner's approval. Computer viruses, spyware, spam, email scams, and phishing are all classified as malware. Viruses are destructive programs that wreak havoc on computer data. Saboteur computer hackers bury virus programs within other harmless data. The delivery method evolves daily. No longer are viruses confined to executable files. Viruses can now invade all forms of media and data. Only through constant upgrades of antivirus programs can users be relatively safe from infection. In a recent case in California, a 20-year-old hacker seized control of hundreds of thousands of Internet-connected computers using the zombie network called a botnet to serve pop-up ads and renting it to people who mounted attacks on websites and sent out spam (Goodin, 2006).

Computer viruses might not be immediately noticed. Some are designed to lie dormant until triggered by a sequence of keystrokes or a date. On November 1, 1988, a person entered a virus that was intended to live innocently and undetected in ARPANET, a U.S. Department of Defense computer network, the original "Internet." A design error in the virus caused it to replicate out of control. It jammed more than 6,000 computers nationwide, including computers at the Rand Corporation, SRI International, Lawrence Livermore Laboratories, the Massachusetts Institute of Technology, and military bases all over the United States. The virus spread by mailing itself to other computers under the auspices of a legitimate user. Because it continued to replicate, all infected computers slowed down and eventually shut down. In the past few years, we have experienced viruses by the names of Klez, Melissa, W32, Blaster, Sasser, Sober, and Michelangelo. The Sobig-F email worm created millions of copies of itself and spread worldwide more rapidly than earlier viruses (see www.pcworld.com/news/article/0,aid,112411,00.asp). W32.Mydoom.A@mm (also known as W32.Novarg.A) is a mass-mailing worm that arrives as an attachment with the file extension .bat, .cmd, .exe, .pif, .scr, or .zip. When a computer is infected, the worm sets up a backdoor into the system by opening TCP ports and can potentially allow an attacker to connect to the computer and use it as a proxy to gain access to its network resources (see http://securityresponse.symantec.com/avcenter/venc/data/w32.novarg.a@mm.html).

Trotter (2003) summarized the cyber virus software intruders as follows:

Backdoor. A secret computer program that gives its creator a method of gaining access without a password to a computer system or computer network, often allowing the infected system to be used in later attacks.
Trojan horse. A program that evades security and masquerades as something harmless. Unlike viruses, Trojan horses do not replicate themselves, but they can be just as destructive.

Virus. A malicious program or piece of software code that attaches itself to a computer program, usually with unwitting assistance from the computer user. Viruses can replicate themselves, which potentially can clog the system until it stops working. Some viruses destroy data, transmit themselves across networks, and bypass security systems.

Worm. A type of virus that can replicate itself over a computer network and usually performs malicious actions, such as using up the computer's resources and potentially shutting the system down. Hybrid worms may contain viruses, backdoors, and Trojan horses (see www.edweek.org/ew/ewstory.cfm?slug=02virus.h23).

Computer viruses are no laughing matter. To combat viruses, antivirus programs detect and eradicate known viruses, and to be effective, these programs must be updated weekly (see the Anti-virus Research Center for more information at www.symantec.com/avcenter).

Spam. Spam (unwanted email such as unsolicited email advertisements) has been increasing at an alarming rate, forcing Congress to begin pursuing legislation to reduce spam. Charp (2003) reported that 49 percent of users spend from 40 minutes a day to almost 4 hours a week deleting spam. Other common terms are cyberslacking which is the overuse of the Internet in the workplace for purposes other than work and cyberharassment that is email that is obscene or hateful or that threatens or frightens and usually has offensive sexist or racist content! See Figure 5.2 for most common email subject lines. Compare 2005 to 2003 to see the changes in spam subject line notes. Many computer users are getting additional email addresses to share with advertisers and thus have protected their personal and business email. Obviously, shared email addresses can end up with unscrupulous advertisers.

Email Scams. In addition to spams and phishing, there are many email scams, as listed in Figure 5.3 (page 116).

Spyware. Spyware refers to malicious software that is designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. There are free spyware detection programs as well as antispyware software programs which will remove and then prevent the malicious spyware. Be sure to keep your computer updated with a spyware checker. Also, keep up with the recommended security updates for the computer's operating system.

Phishing. Phishing is a term used to describe the action of assuming the identity of a legitimate organization or website, using forged email or web pages and with a view to convince consumers to share their user names, passwords, and personal financial information. How to avoid phishing scams is often referred to as spear-phishing (www.aol.com/creditcard2003.html). Be sure to check credit card bills and respond to phishing scams by contacting the credit card company immediately. How to respond to phishing scams is often referred to as spear-phishing.
financial information for the purpose of using it to commit fraud. Phishing is also often referred to as identity theft (www.millersmiles.co.uk/identitytheft/phishing.html). By hijacking the trusted brands of well-known banks, online retailers, and credit card companies, phishers are able to convince up to 5 percent of recipients to respond to them (see www.antiphishing.org). A more recent form of phishing is spear-phishing, which targets corporations (Vamosi, 2005).

How to Avoid Phishing Scams. The number and sophistication of phishing scams sent out to consumers is continuing to increase dramatically. While ecommerce is very safe, as a general rule you should be careful about giving out your personal financial information over the Internet. JPMorgan Chase has compiled a list of recommendations that you can use to avoid becoming a victim of these scams.
FIGURE 5.3  Top ten internet frauds listed by the National Consumers League.

1. Bogus online auctions, where the items purchased are never delivered.
2. Deliberate misrepresentation or nondelivery of general merchandise purchased online.
3. Nigerian money offers.
4. Deliberate misrepresentation or nondelivery of computer equipment or software purchased online.
5. Internet access scams, where bogus Internet service providers fraudulently charge for services that were never ordered or received.
6. Credit card or telephone charges for services that were never ordered or misrepresented as free. These often include charges for accessing “adult” material.
7. Work-at-home schemes promising wildly exaggerated sales and profits.
8. Advance fee loans, where consumers are duped into paying upfront charges for loans which never materialize.
9. Phony offers of cheap-rate credit card deals, once again on payment of upfront fees.
10. Business opportunities or franchises sold on the basis of exaggerated profit.

See also http://news.bbc.co.uk/1/hi/business/2003264.stm.
Source: www.nclnet.org


• Be suspicious of any email with urgent requests for personal financial information.
• Unless the email is digitally signed, you can’t be sure it wasn’t forged or spoofed.
• Phishers typically include upsetting or exciting (but false) statements in their emails to get people to react immediately.
• They typically ask for information such as user names, passwords, credit card numbers, Social Security numbers, and so forth.
• Phisher emails are NOT typically personalized, while valid messages from your bank or ecommerce company would be personalized.
• Don’t use the links in an email to get to any web page if you suspect the message might not be authentic.
• Call the company on the telephone, or log onto the website directly by typing in the web address in your browser.
• Avoid filling out forms in email messages that ask for personal financial information.
• You should only communicate information such as credit card numbers or account information via a secure website or telephone.
• Always ensure that you’re using a secure website when submitting credit card or other sensitive information via your web browser.
• To ensure that you are on a secure web server, check the beginning of the web address in your browser’s address bar; it should be “https://” rather than just “http://”.
• Regularly check your online accounts as well as bank, credit, and debit card statements to ensure that all transactions are legitimate.
• Ensure that your browser is up to date and that all security patches are applied.
  • Microsoft Internet Explorer: www.microsoft.com/security
  • Mozilla and Firefox: www.mozilla.org/security/shell.html
• Always report phishing or spoofed emails to the following groups:
  • Federal Trade Commission at spam@uce.gov
  • Internet Fraud Complaint Center of the FBI at www.ifccfbi.gov

**Gaining Identity Information through Phishing.** An identity thief who allegedly used hijacked corporate logos and deceptive spam to con consumers out of credit card numbers and other financial data has agreed to settle Federal Trade Commission (FTC) charges that his scam violated federal laws. If approved by the court, the defendant, a minor, will be barred for life from sending spam and will give up his ill-gotten gains. The FTC alleged that the scam worked like this: Posing as America Online, the con artist sent consumers email messages claiming that there had been a problem with the billing of their AOL account. The email warned consumers that if they did not update their billing information, they risked losing their AOL account and Internet access. The message directed consumers to click on a hyperlink in the body of the email to connect to the “AOL Billing Center.” When consumers clicked on the link, they landed on a site that contained AOL’s logo, AOL’s type style, AOL’s colors, and links to real AOL web pages. It appeared to be AOL’s Billing Center. But it was not. The defendant had hijacked AOL’s identity and was going to use it to steal consumers’ identities, as well, the FTC alleged (FTC, 2003).

**Social Engineering**

Mossberg (2006) provides an excellent list of tips to help you avoid the latest theft scams which he calls “social engineering.” He defines social engineering as consisting of tactics that try to fool users into giving up sensitive financial data that criminals can use to steal their money and even their identities. He includes “phishing,” the practice by which crooks create emails and websites that look just like legitimate messages and sites from real banks and other financial companies as social engineering and is linked to a category of malicious software called Crimeware—programs that help criminals steal your private financial information. These terms are confusing and overlapping, but the threat is real. Increasingly, common-looking scams are combined with secret installations of software that help criminals spy on you and steal your data. Mossberg provides the following tips (http://online.wsj.com/article/personal_technology.html?mod=djemptech):
1. Don’t trust email from financial institutions. Email is so easily manipulated by crooks that you simply should never, ever consider any email from a financial institution as legitimate. The message may bear a bank’s or a broker’s logo, but you should never respond to such an email, and never click on any link it contains. There is a very high chance it’s a skillful fraud and that the link will take you to a clever fake website designed to capture passwords and account numbers. The site may also silently install on your PC a program called a key logger, which records everything you type and sends that information back to the crooks.

2. Never respond to unsolicited commercial email, or spam, or even click on a link in an unsolicited commercial email. In the old days, responding to spam just got you on more spam email lists. Today, it might also result in the secret installation of a key logger or other malicious software. Besides, any company that has to resort to spam as a sales tool isn’t likely to have a very good product to offer. Moreover, nobody in Nigeria needs your bank account to store stolen millions. Would you buy a stock touted on the street by a complete stranger? If not, why would you buy one touted in a spam email? The only safe response to spam is to ignore it and delete it.

3. Don’t download or use free software unless you’re sure it’s legitimate. Sites offering free cursors, for instance, can secretly install all sorts of bad stuff on your PC. This is especially true of free security software, which is sometimes just malicious software posing as a security program. If you suddenly see a security program pop up on your PC, don’t trust it.

**MAINTAINING SECURITY**

The need for security of computer equipment and computer data is significant for a computer system of any size, from a large mainframe system with extensive peripheral equipment to a single computer on a student’s desk. Security measures prevent the fraudulent use or destruction of computer equipment. These measures include something a person has (a key or badge), something a person knows (a password), or something about a person (a fingerprint, a voiceprint, a facial feature).

Most large companies have security systems that one must pass through to gain access to the computer room. These systems may use special cards to insert or buttons to press on the outer door of the computer room. Other security measures include allowing only the personnel necessary to perform certain functions to be in a certain place, for instance, in the computer room. Therefore, once programs are written and in place, computer programmers should not be allowed to go into the computer room and should never be allowed to run their programs. Whereas it is reasonable in large organizations to allow only authorized personnel to enter the computer room, in most schools such a security measure would be unrealistic. However, access to the administrative computer containing confidential records should be limited. Security measures in the computer lab and in individual classes should
be necessarily broader. Another measure requires the investigation of staff and security clearances for those who work with confidential information. A third measure establishes a system for efficiently investigating suspected breaches of security. No system is ever foolproof, but every effort should be made to ensure the security of both computer and data.

Biometric devices are now being used to ensure privacy, protect assets, confirm identity, and guard against unauthorized access. Biometric devices scan body parts such as fingerprints or retinas. A "smart card" is a plastic credit card type device with an embedded integrated circuit for storing information. Biometric technologies and smart cards are replacing the antiquated method of using passwords or PIN numbers. Electronic signatures, or e-signatures, represent a new form of technology used to verify a party's identity so as to certify contracts that are agreed to over the Internet. See Figures 5.4 and 5.5 for listings of security technologies and financial losses as reported by the FBI in a 2005 Crime Survey.

**FIGURE 5.4** | Security technologies used.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewalls</td>
<td>97%</td>
</tr>
<tr>
<td>Anti-virus software</td>
<td>96%</td>
</tr>
<tr>
<td>Intrusion Detection Systems</td>
<td>72%</td>
</tr>
<tr>
<td>Server-based access control lists</td>
<td>70%</td>
</tr>
<tr>
<td>Encryption for data in transit</td>
<td>68%</td>
</tr>
<tr>
<td>Reusable account/login passwords</td>
<td>52%</td>
</tr>
<tr>
<td>Encrypted files</td>
<td>46%</td>
</tr>
<tr>
<td>Smart cards/other one-time password tokens</td>
<td>42%</td>
</tr>
<tr>
<td>Public Key Infrastructure</td>
<td>35%</td>
</tr>
<tr>
<td>Intrusion Prevention Systems</td>
<td>35%</td>
</tr>
<tr>
<td>Biometrics</td>
<td>15%</td>
</tr>
</tbody>
</table>

FIGURE 5.5 | Dollar amount losses by type.

![Table of Dollar Amount Losses By Type](image)


INDIVIDUAL PRIVACY

Our digital identities are being stored in databases of companies we've never heard of. Private information is not only being captured online via the Internet, it is being collected in our offline world as well. Buying patterns are data mined from point-of-sale terminals via your supermarket club card. Advancements in biometric scanning technologies warrant a closer examination of our networked world of private information.

Until 1974, there was little concern about privacy with regard to databases. Few databases shared their information because access was slow and inefficient. However, as technology advanced and databases evolved into data warehouses, concern for individual privacy increased. President Gerald Ford signed the Privacy Act of 1974 into law. Its purpose was to protect confidentiality of files generated by the federal government. Its principles are paraphrased as follows:
• There must be no personal data record-keeping systems whose very existence is secret.
• There must be a way for individuals to find out what information about them is in a record and how it is used.
• There must be a way for individuals to prevent information about them obtained for one purpose from being used or made available for other purposes without their consent.
• There must be a way for individuals to correct or amend records of identifiable information about them.
• Organizations creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

Let's examine the privacy issue with regard to several situations. First, consider credit checks. Today, we are a nation of borrowers. In fact, we have become so dependent on credit that business probably could not exist without it. Cars are bought on time payments, merchandise is charged to credit cards, and homes are mortgaged. All these items are bought on deferred payment plans requiring the establishment of credit.

Problems always arise whenever there is access to credit information. Questions range from who is authorized to access the information to how much information that person is entitled to know. In addition, the information available may or may not be accurate. For example, data might have been entered incorrectly, resulting in denial of credit purchases. Often, information is entered into a system but is never removed. A record of an arrest in a law enforcement database may be entered without indication of whether the person was acquitted of the charge. This same information may result in a university refusing an applicant admission. Another problem results from the unrestricted use of data. The large amounts of data available today often become accessible to more people than originally intended. The growth of government obviously increases the amount of data collected. In addition, data collected by one agency is often shared and used by other agencies for other purposes.

Tax forms are submitted to the Internal Revenue Service each year. The Census Bureau gathers information and law enforcement databases compile criminal records. Motor vehicle departments annually update data on registered car owners and licensed drivers, and voter registration lists abound. With this wide range of available information, these databases could be merged into data warehouses. These mergers could produce a detailed picture of an individual, threatening the individual's right to privacy. Many doctors and other professionals are reluctant to store client information in computer systems because of such a threat.

The shift to networked information environments challenges privacy in additional ways. Some popular email systems allow senders of bulk commercial email to track email recipients' web browsing behavior. Web browser cookies help companies match website visitors with their email addresses. When you receive an email
message containing a graphic from a website, an email security loophole allows you
to be assigned a unique serial number in a cookie, which is a text file stored in your
hard drive and readable by other computers. This serial number or cookie is stealth­
ily transmitted as you browse the web.

Technological advances are increasingly undermining privacy. Safeguarding our
privacy is therefore a major issue requiring a thorough understanding of who is
warehousing data, for what purpose, and how personal information is collected
without our consent. The computer is invaluable in the management and distribu­
tion of information. However, it is up to those with access to this information to use
it legally, wisely, and ethically. A strong need exists for improved oversight and
stricter enforcement of current laws. To ensure that legal protections are not ignored,
a public research center, the Electronic Privacy Information Center (EPIC), estab­
lished a website at www.epic.org to disseminate information on emerging civil lib­
erties issues, including privacy and First Amendment concerns.

Privacy issues are increasingly a concern for educators as well. The handling of
student information is protected under the Family Educational Rights and Privacy
Act (FERPA) of 1974. This federal law provides parents and students with the right
to see their school records and to request corrections to records believed to be inac­
curate or misleading. Schools must have written consent from parents or an eligible
student (18 years or older) before releasing any information on a student. However,
exceptions exist for certain entities, for instance, school employees or a contract
agency conducting a study.

So far, our discussion of computer crimes and threats to privacy illustrates some
of the drastic changes computers are causing in our society. Another key set of is­
issues, ethics and equity, impacts new responsibilities facing educators. The next two
sections explore these concerns in education.

I ETHICAL AND LEGAL CONCERNS IN EDUCATION

Educators share with parents and society the task of teaching ethical use of comput­
ers and the Internet. To help teachers develop a set of ethics applicable to computer
and Internet use, schools create and implement an acceptable use policy (AUP). The
AUP is a critical part of the school’s technology plan and states the rules governing
computer and Internet use and the consequences for violations. Parents and their

Do Ken

KenRa

Bloor

female

crime,

buyin

Privacy issues are increasingly a concern for educators as well. The handling of
student information is protected under the Family Educational Rights and Privacy
Act (FERPA) of 1974. This federal law provides parents and students with the right
to see their school records and to request corrections to records believed to be inac­
curate or misleading. Schools must have written consent from parents or an eligible
student (18 years or older) before releasing any information on a student. However,
exceptions exist for certain entities, for instance, school employees or a contract
agency conducting a study.

So far, our discussion of computer crimes and threats to privacy illustrates some
of the drastic changes computers are causing in our society. Another key set of is­
issues, ethics and equity, impacts new responsibilities facing educators. The next two
sections explore these concerns in education.

I ETHICAL AND LEGAL CONCERNS IN EDUCATION

Educators share with parents and society the task of teaching ethical use of comput­
ers and the Internet. To help teachers develop a set of ethics applicable to computer
and Internet use, schools create and implement an acceptable use policy (AUP). The
AUP is a critical part of the school’s technology plan and states the rules governing
computer and Internet use and the consequences for violations. Parents and their

Do Ken

KenRa

Bloor

female

crime,

buyin

Privacy issues are increasingly a concern for educators as well. The handling of
student information is protected under the Family Educational Rights and Privacy
Act (FERPA) of 1974. This federal law provides parents and students with the right
to see their school records and to request corrections to records believed to be inac­
curate or misleading. Schools must have written consent from parents or an eligible
student (18 years or older) before releasing any information on a student. However,
exceptions exist for certain entities, for instance, school employees or a contract
agency conducting a study.

So far, our discussion of computer crimes and threats to privacy illustrates some
of the drastic changes computers are causing in our society. Another key set of is­
issues, ethics and equity, impacts new responsibilities facing educators. The next two
sections explore these concerns in education.

I ETHICAL AND LEGAL CONCERNS IN EDUCATION

Educators share with parents and society the task of teaching ethical use of comput­
ers and the Internet. To help teachers develop a set of ethics applicable to computer
and Internet use, schools create and implement an acceptable use policy (AUP). The
AUP is a critical part of the school’s technology plan and states the rules governing
computer and Internet use and the consequences for violations. Parents and their

Do Ken

KenRa

Bloor

female

crime,

buyin

Privacy issues are increasingly a concern for educators as well. The handling of
student information is protected under the Family Educational Rights and Privacy
Act (FERPA) of 1974. This federal law provides parents and students with the right
to see their school records and to request corrections to records believed to be inac­
curate or misleading. Schools must have written consent from parents or an eligible
student (18 years or older) before releasing any information on a student. However,
exceptions exist for certain entities, for instance, school employees or a contract
agency conducting a study.

So far, our discussion of computer crimes and threats to privacy illustrates some
of the drastic changes computers are causing in our society. Another key set of is­
issues, ethics and equity, impacts new responsibilities facing educators. The next two
sections explore these concerns in education.

I ETHICAL AND LEGAL CONCERNS IN EDUCATION

Educators share with parents and society the task of teaching ethical use of comput­
ers and the Internet. To help teachers develop a set of ethics applicable to computer
and Internet use, schools create and implement an acceptable use policy (AUP). The
AUP is a critical part of the school’s technology plan and states the rules governing
computer and Internet use and the consequences for violations. Parents and their

Do Ken

KenRa

Bloor

female

crime,

buyin

Privacy issues are increasingly a concern for educators as well. The handling of
student information is protected under the Family Educational Rights and Privacy
Act (FERPA) of 1974. This federal law provides parents and students with the right
to see their school records and to request corrections to records believed to be inac­
curate or misleading. Schools must have written consent from parents or an eligible
student (18 years or older) before releasing any information on a student. However,
exceptions exist for certain entities, for instance, school employees or a contract
agency conducting a study.

So far, our discussion of computer crimes and threats to privacy illustrates some
of the drastic changes computers are causing in our society. Another key set of is­
issues, ethics and equity, impacts new responsibilities facing educators. The next two
sections explore these concerns in education.

I ETHICAL AND LEGAL CONCERNS IN EDUCATION

Educators share with parents and society the task of teaching ethical use of comput­
ers and the Internet. To help teachers develop a set of ethics applicable to computer
and Internet use, schools create and implement an acceptable use policy (AUP). The
AUP is a critical part of the school’s technology plan and states the rules governing
computer and Internet use and the consequences for violations. Parents and their

Do Ken

KenRa

Bloor

female

crime,

buyin

Privacy issues are increasingly a concern for educators as well. The handling of
student information is protected under the Family Educational Rights and Privacy
Act (FERPA) of 1974. This federal law provides parents and students with the right
to see their school records and to request corrections to records believed to be inac­
curate or misleading. Schools must have written consent from parents or an eligible
student (18 years or older) before releasing any information on a student. However,
exceptions exist for certain entities, for instance, school employees or a contract
agency conducting a study.

So far, our discussion of computer crimes and threats to privacy illustrates some
of the drastic changes computers are causing in our society. Another key set of is­
issues, ethics and equity, impacts new responsibilities facing educators. The next two
sections explore these concerns in education.

I ETHICAL AND LEGAL CONCERNS IN EDUCATION

Educators share with parents and society the task of teaching ethical use of comput­
ers and the Internet. To help teachers develop a set of ethics applicable to computer
and Internet use, schools create and implement an acceptable use policy (AUP). The
AUP is a critical part of the school’s technology plan and states the rules governing
computer and Internet use and the consequences for violations. Parents and their
children are held responsible to adhere to this policy. There are many commercial software products that parents can use to screen their children's Internet access including messaging and chat rooms. In fact, most products can limit access to certain times of day and also have the ability to keep logs of the websites their children have visited. Do students know what is legal to copy and what is not legal to copy? The following are the results of a recent poll attempting to answer this question.

Do Kids Care If It's Illegal?

KenRadio.com (2006) reports that a poll recently conducted by the LA Times and Bloomberg found that the majority of teenagers and young adults, both male and female, up to the age of 24, believe that while copying stolen music or movies is a crime, copying purchased CDs or DVDs is not. These young consumers know that downloading free music and movies from unauthorized sites is illegal. They know buying bootlegged CDs and DVDs is wrong, too. But, according to the survey, 60 to 70 percent of them think it is perfectly all right to burn discs for or from friends, as long as the discs were legitimately purchased. As far as lawyers for the music and film industries are concerned, copying a CD or DVD for even one friend, even if you purchased it and paid full price, violates the federal copyright code and it is a crime. Young users do not agree. See Table 5.1.

KenRadio.com also explained that the results of the poll implied that 69 percent of teens ages 12 to 17 believe it is legal to copy a CD from a friend who purchased the original, but only 21 percent feel it is legal to copy a CD if a friend obtained the music for free. Similarly, 58 percent think it is legal to copy a DVD or videotape that a friend purchased, but only 19 percent think copying is legal if the material wasn’t legitimately bought. In another study, earlier this year, Harris Interactive found that

<table>
<thead>
<tr>
<th>Table 5.1</th>
<th>U.S. Net Users Who Believe That It Is a Crime</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>12-14</td>
</tr>
<tr>
<td>Copy a CD from a friend who paid for it</td>
<td>27%</td>
</tr>
<tr>
<td>Copying a DVD/VHS from a friend who paid for it</td>
<td>39%</td>
</tr>
<tr>
<td>Download free music from an unauthorized site</td>
<td>79%</td>
</tr>
<tr>
<td>Download free movies from an unauthorized site</td>
<td>83%</td>
</tr>
<tr>
<td>Buying a bootleg CD</td>
<td>82%</td>
</tr>
<tr>
<td>Buying a bootleg DVD/VHS</td>
<td>83%</td>
</tr>
<tr>
<td>Shoplifting an item worth less than $20</td>
<td>97%</td>
</tr>
<tr>
<td>Shoplifting an item worth more than $20</td>
<td>99%</td>
</tr>
</tbody>
</table>

Source: [http://KenRadio.com](http://KenRadio.com)
illegal downloading of music, movies, games, and software by young users was trending downward. See Figure 5.6.

COPYRIGHT

Teachers are role models. Therefore, there is no substitute for ethical teacher behavior and proper supervision of students. Teachers must set an example of ethical behavior whenever using or discussing computers. A lecture on the evils of software piracy becomes meaningless if the teacher practices piracy. Understanding current copyright issues and the term educational fair use are paramount to teachers’ ethical behavior.

The federal agency charged with administering the copyright law is the Copyright Office of the Library of Congress. (Visit its site at http://lcweb.loc.gov/copyright/title17 to review the law, or www.loc.gov/copyright/circs/circ1.html to review the basics.) A copyright gives the creator the exclusive right to reproduce, distribute, perform, display, or license his or her work. When the original work is “fixed” in a “tangible medium of expression,” copyright is automatic and notice is not necessary. For example, the email you write is copyrighted. Copyright protection lasts the lifetime of the creator plus 70 years; however, limited exceptions exist for types of fair use.
Fair use is defined in Section 107 of the 1976 Copyright Act (see www.loc.gov/copyright/title17/92chap1.html#107). Use for criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research is not an infringement of copyright. To determine whether a use is fair under the above law, the following factors must be considered but are not limited to:

- The purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes
- The nature of the copyrighted work
- The amount and substantiality of the portion used in relation to the copyrighted work as a whole
- The effect of the use upon the potential market for or value of the copyrighted work

Digital Millennium Copyright Act

In 1998 the Digital Millennium Copyright Act (DMCA) was signed into law. The DMCA's purpose is to update our copyright law for the digital age. An overview of the DMCA can be found at www.asu.edu/counsel/brief/dig.html. Under federal copyright law, no copyrighted work may be copied, published, disseminated, displayed, performed, or played without permission of the copyright holder except in accordance with fair use or licensed agreement. This includes music, movies, and other copyrighted material.

Teach Act of 2002

On November 2, 2002, the Teach Act of 2002 was signed into law (www.copyright.gov/legislation/pl107-273.pdf#13210). The Teach Act of 2002 requires the use of technological measures that reasonably prevent further copying and distribution of copyrighted works. A class is limited to access to copyrighted works only for those officially enrolled. In addition, the access is only for the time period necessary to complete the class session. Finally, the digital transmissions are expected not to interfere with technological measures used by the copyright owners to prevent such retention or unauthorized further dissemination. The Association of Research Libraries website at www.arl.org/info/frn/copy/copytoc.html is a good source to acquire current and accurate information on copyright issues.

Copyright and Fair Use Guidelines for Teachers

Davidson (2005) developed the chart in Table 5.2 to inform classroom teachers of their rights under the copyright law and copyright guidelines of the United States. Copyright and the notion of intellectual property was written into the Constitution of the United States to promote learning and the useful arts—and was designed to be supportive of the work of educators.
The purpose of copyright protection is repeatedly and mistakenly reported to be for the protection of authors and other intellectual property owners. In fact, copyright has been always been for the purpose of benefiting society as a whole and particularly the institutions of education. Learning, or science, in the language of the Enlightenment and the Constitution, was to be promoted by allowing authors and others rights for a limited time for their work. The first copyright act written into federal law was titled “The Education Act.”

Teachers in the classroom make the decisions closest to the field of instruction, and it is teachers who have been given the greatest rights—rights that even their districts do not have. Hall Davidson, a teacher, designed a Copyright Chart to inform teachers of what they may do under the law. A PDF form of the chart is available at www.mediafestival.org/downloads.html. See Table 5.2.

### Restricting Access to Harmful Material

The Child Online Protection Act (COPA), enacted in 1998, replaced the Communication Decency Act and bans sending harmful materials to minors as well as underage exposure to sexually explicit materials. The Children’s Online Privacy Protection Act (COPPA), which went into effect on April 21, 2000 (47 U.S.C. §231), applies to the online collection of personal information from children under 13. It explains what a website operator must include in a privacy policy, when and how to seek verifiable consent from a parent, and what responsibilities an operator has to protect children’s privacy and safety online (see www.ftc.gov/bcp/online/pubs/buspubs/coppa.htm).

COPA imposes a $50,000 fine and 6 months in prison for the knowing posting, for “commercial purposes,” of World Wide Web content that is “harmful to minors,” but provides an affirmative defense to commercial web speakers who restrict access to prohibited materials by “requiring use of a credit card” or “any other reasonable measures that are feasible under available technology,” §231(c)(1). COPA was enacted in response to Reno v. American Civil Liberties Union, 521 U.S. 844, in which this Court held that the Communications Decency Act of 1996, Congress’ first attempt to make the Internet safe for minors by criminalizing certain Internet speech, was unconstitutional because it was not narrowly tailored to serve a compelling governmental interest and because less restrictive alternatives were available. Respondents, who were web speakers and others concerned with protecting the freedom of speech, filed suit for a preliminary injunction against COPA’s enforcement.

After considering testimony presented by both respondents and the government, the District Court granted the preliminary injunction, concluding that respondents were likely to prevail on their argument that there were less restrictive alternatives to COPA, particularly blocking or filtering technology. The Third Circuit affirmed on different grounds, but this Court reversed Ashcroft v. American Civil Liberties Union, 535 U.S. 564.

On remand, the Third Circuit again affirmed, concluding that COPA was not the least restrictive means available for the government to serve the interest of preventing minors from using the Internet to gain access to harmful materials (U.S. Supreme Court decision No. 03—218. Argued March 2, 2004—Decided June 29, 2004). For more information, see http://supct.law.cornell.edu/supct/html/03-218.ZS.html and www.epic.org/free_speech/copa.
In the letter to Congressional Subcommittee Chair Kastenmeier dated 3/19/76 summarizing many of the agreements [below], representatives of the Ad Hoc Committee of Educational Institutions and Organizations of Copyright Law Revision and the Authors League of America, Inc., and the Association of American Publishers, Inc., state that these guidelines were "not intended to limit the types of copying permitted under the standards of fair use under judicial decision and which are stated in Section 107 of the Copyright Revision Bill. There may be instances in which copying which does not fall within the guidelines stated [below] may nonetheless be permitted under the criterion of fair use."

For more detailed information and references on copyright, (see [www.mediafestival.org/downloads.html#anchor359082](http://www.mediafestival.org/downloads.html#anchor359082)). A pdf version of this chart is also available for download.

### Table 5.2 Classroom Copyright Chart

<table>
<thead>
<tr>
<th>Printed Material</th>
<th>What You Can Do</th>
<th>According to</th>
<th>The Fine Print</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poem less than 250 words</td>
<td>Teachers may make multiple copies for classroom use.</td>
<td>United States Copyright Office Circular 21</td>
<td>No more than one copy per student. Usage must be: At the &quot;instance and inspiration of a single teacher&quot; and when the time frame doesn't allow enough time for asking permission. Only for one course in the school. No more than nine instances per class per term. (Current news publications such as newspapers can be used more often). Don't create anthologies. &quot;Consumables&quot; can't be copied. Don't do it every term. If time allows, seek permission. Can't be directed by &quot;higher authority.&quot; Copying can't be substitute for buying. Copies may be made only from legally acquired originals.</td>
</tr>
<tr>
<td>Excerpt of 250 words from a poem greater than 250 words</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Articles, stories, or essays less than 2,500 words</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Excerpt from a longer work (10% of work or 1,000 words, whichever is less— but a minimum of 500 words)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>One chart, diagram, graph, cartoon, or picture per book or per periodical issue</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Two pages (max) from an illustrated work less than 2,500 words (like children's books)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(continued)
<table>
<thead>
<tr>
<th>Printed Material (continued)</th>
<th>What You Can Do</th>
<th>According to</th>
<th>The Fine Print</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A chapter from a book</td>
<td>Teachers may make a single copy for teacher use for research or lesson preparation.</td>
<td>United States Copyright Office Circular 21</td>
<td>Same as above.</td>
</tr>
<tr>
<td>• An article from a periodical</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Short story, short essay, or short poem</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Chart, graph, diagram, drawing, cartoon, picture from a book, periodical, or newspaper</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Portions of a work</td>
<td>A librarian may make up to three copies “solely for the purpose of replacement of a copy ... that is damaged, deteriorating, lost or stolen”</td>
<td>Section 108 Copyright Act (1976) as amended by the Digital Millennium Copyright Act</td>
<td>The library must first determine that after “reasonable investigation that copy ... cannot be obtained at a fair price” or that the format is obsolete.</td>
</tr>
<tr>
<td>• An entire work</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• A work if “the existing format in which a work is stored has become obsolete”</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Text for Use in Multimedia Projects**

<table>
<thead>
<tr>
<th></th>
<th>What You Can Do</th>
<th>According to</th>
<th>The Fine Print</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Same rights as &quot;Printed Material&quot; above</td>
<td>Students may incorporate text in multimedia projects. Teachers may incorporate into multimedia for teaching courses.</td>
<td>Fair Use Guidelines for Educational Multimedia</td>
<td>Teachers may use for two years, after that permission is required. Students may keep in portfolio for life.</td>
</tr>
</tbody>
</table>

**Illustrations and Photographs**

<table>
<thead>
<tr>
<th></th>
<th>What You Can Do</th>
<th>According to</th>
<th>The Fine Print</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Photograph</td>
<td>Single works may be used in their entirety but not more than five images by an artist or photographer. From a collection, not more than fifteen images or 10%, whichever is less.</td>
<td>Fair Use Guidelines for Educational Multimedia</td>
<td>Older images may be in the public domain, but the collection may be copyrighted.</td>
</tr>
<tr>
<td>• Illustration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Collections of photographs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Collections of illustrations</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 5.2 Continued

<table>
<thead>
<tr>
<th>Video</th>
<th>What You Can Do</th>
<th>According to</th>
<th>The Fine Print</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video (&quot;Motion Media&quot;) for Use in Multimedia Projects</td>
<td>Students &quot;may use portions of lawfully acquired copyrighted works in their academic multimedia,&quot; defined as 10% or three minutes (whichever is less) of &quot;motion media.&quot;</td>
<td>Fair Use Guidelines for Educational Multimedia</td>
<td>&quot;Proper attribution and credit must be noted for all copyrighted works included in multimedia, including those prepared under fair use&quot; (Tina Ivany, UC San Diego, 12/08/95).</td>
</tr>
<tr>
<td>Video for Integration into Video Projects</td>
<td>Students &quot;may use portions of lawfully acquired copyrighted works in their academic multimedia.&quot;</td>
<td>Fair Use Guidelines for Educational Multimedia</td>
<td>The material must be legitimately acquired (a legal copy, not bootleg or home recording).</td>
</tr>
</tbody>
</table>

(continued)
### TABLE 5.2 Continued

<table>
<thead>
<tr>
<th>Music for Integration into Multimedia/Video Projects</th>
<th>What You Can Do</th>
<th>According to</th>
<th>The Fine Print</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Music</td>
<td>Up to 10% of a copyrighted musical composition may be reproduced, performed, and displayed as part of a multimedia program produced by an educator or student for educational purposes.</td>
<td>Fair Use Guidelines for Educational Multimedia</td>
<td>Some authorities cite a maximum length of 30 seconds (<a href="http://www.indiana.edu">www.indiana.edu</a>), some do not mention a maximum (Tina Ivany, UCSD, 12/08/95). See below.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Computer Software</th>
<th>What You Can Do</th>
<th>According to</th>
<th>The Fine Print</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Purchased software</td>
<td>Software may be lent by the library. Software may be installed at home and at school. Software may be installed on multiple machines. Software may be copied for archival use to replace lost, damaged, or stolen copies. Software can be distributed to users via a network. Librarians may make archival copies.</td>
<td>Sections 107 and 108 of Copyright Act and subsequent amendments</td>
<td>Take aggressive action to monitor that copying is not taking place (for retention). Only one machine at a time may use the program. The number of machines being used must never exceed the number of licensed. If unavailable at fair price or is an obsolete format. The number of simultaneous users must not exceed the number of licenses. A network license may be required for multiple users.</td>
</tr>
<tr>
<td>• Licensed software</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Internet
- Internet
- World Wide Web

### Television
- Broadcast TV: ABC, CBS, NBC, UPN, Fox
- Cable TV: CNN, MTV, HBO (etc.)
- Tapes may be recorded from broadcasts.
**TABLE 5.2 Continued**

<table>
<thead>
<tr>
<th>Internet</th>
<th>What You Can Do</th>
<th>According to</th>
<th>The Fine Print</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Internet connections</td>
<td>Images may be downloaded for student projects. Material may be uploaded temporarily to a website password restricted to students. Do not archive the materials. Sound files may be downloaded for use in projects (see portion restrictions above).</td>
<td>Fair Use Guidelines for Educational Multimedia &amp; DMCA</td>
<td>Images may not be reposted onto the Internet without permission. Sound or music files may not be copied and posted on the Internet without permission.</td>
</tr>
<tr>
<td>• World Wide Web</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Television</th>
<th>What You Can Do</th>
<th>According to</th>
<th>The Fine Print</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Broadcast (e.g., ABC, NBC, CBS, UPN, PBS, local television stations)</td>
<td>Live “off the air” broadcasts may be used for instruction. Tapes made from broadcasts may be used for instruction.</td>
<td>Congress</td>
<td>Things get interesting when you want to retain tapes. Minimum rights allow for ten school days. Enlightened rights holders often allow for much more. PBS series Reading Rainbow offers three year retention rights, for example. If you like it enough to keep it more than three years, buy it!</td>
</tr>
<tr>
<td>• Tapes made from broadcast</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cable Television</th>
<th>What You Can Do</th>
<th>According to</th>
<th>The Fine Print</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CNN</td>
<td>May be used with permission. Many programs may be retained for years—depending on the program. Check with Cable in the Classroom. <a href="http://www.ciconline.org/main.cfm">www.ciconline.org/main.cfm</a></td>
<td>Cable systems (and their associations)</td>
<td>The guidelines for television programs were defined by Congress before cable television was a factor. Cable programs are not technically covered by the same guidelines as broadcast television.</td>
</tr>
<tr>
<td>• MTV</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• HBO (etc.)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Tapes made from cable</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(continued)
Table 5.2 Continued

<table>
<thead>
<tr>
<th>Film or Filmstrip</th>
<th>What You Can Do</th>
<th>According to</th>
<th>The Fine Print</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 16 millimeter films</td>
<td>“Teachers may duplicate a single copy of a small portion... for teaching purposes.”</td>
<td>Copyright Policy and Guidelines for California’s School Districts, California Department of Education</td>
<td>These must be films or filmstrips that you own.</td>
</tr>
<tr>
<td>• filmstrips</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Return for updates to: www.mediafestival.org/copyrightchart.html  Hall Davidson  hall@cccd.edu

Plagiarism

Another growing concern among educators is Internet plagiarism. Finding information on the Internet makes verbatim text, enhanced photos, and animations very convenient for students to cut and paste into their papers and research reports. Even entire essays can be downloaded and passed off as original works. Entrepreneurs can acquire a repository of essays and research papers for resale. In less than a second after entering the search word essays into Google or Yahooligans, you can find many websites listing student essays! Because so many sources of information are available on the Internet, plagiarizing the information in papers and reports is a temptation. See Chapter 15 and www.plagiarism.org/index.html for more information on this topic.

Information Accuracy

Another growing concern among educators is the accuracy of Internet-provided information. There are no standards or clearinghouses to screen the plethora of information available. Careful review of all Internet information is required.

Role-Playing Models for Ethical Behavior

These are a few of the technology-related issues. Teachers can spend class time discussing ethical issues with students. There are many role-playing models that cast students as software pirates, software publishers, and so on. Giving students opportunities to role play and discuss these issues helps them develop and clarify their own ethical codes. See www.vuw.ac.nz/staff/alastair_smith/evaln and www.library.jhu.edu/researchhelp/general/evaluating.

Kid Safety and Cybersafety

Child safety, often referred to as Kid Safety or Cybersafety, is the goal of parents, teachers, and schools. The Internet Keep Safe Coalition group teaches basic rules...
Governors and/or their spouses formed this coalition in partnership with a growing list of crime prevention organizations, law enforcement agencies, foundations, and corporate sponsors. Studies show that one in five youth using the Internet receive an online sexual solicitation in a 1-year period, and 29 percent of children will freely give out their home address if asked (retrieved from the www.ikeepsafe.org site on August 10, 2006).

**Helpful Sites for Assistance with Kid Safety**

- Advance notice of bad or offensive sites: www.siteadvisor.com, www.scandoo.com
- Internet protection for web, email, and desktop: www.surfcontrol.com
- Faux Paw’s adventures in storybooks, an animated video download, and educational games: www.ikeepsafe.org/iksc_educators/educational-materials.php
- Educational materials, including worksheets and tests, are available for parents and educators: www.ikeepsafe.org/iksc_educators/educational-materials.php
- Safe email for students: www.gaggle.net

**Social Networking**

Social Networking is growing very rapidly in popularity. There seem to be new sites every few weeks. Angwin (2006) relates senior year notes in the school yearbook to social networking on the computer. Students wrote about what their future profession would be in as well as references to favorite music, sports, and anything they wanted to be remembered by. Members of the networks usually share information with stories, photos, addresses and whatever else is the focus of the particular network. Most of the sites are free.

Unpleasant problems have occurred due to the information provided to the sites including sexual assaults and invasions of privacy. Teachers, parents, and schools now have become aware of some of these unsafe environments and are providing student awareness discussions. Basically, information needs to be provided to help parents and teachers teach their children not to put identifying personal details on their web pages (Barrett, 2006). Some sites now provide safety tips. Following is a list of some of the more popular sites:

**Popular Social Networking Sites**

- 360 Yahoo
  - http://360.yahoo.com
43 Things: What do you want to do with your life?
http://www.43things.com
Blogger
http://blogger.com/start
Bolt
www.Bolt.com
Classmates
www.classmates.com
Facebook
www.myspace.com
Flickr
www.flickr.com
Livejournal
www.livejournal.com
MSN Photo Album
http://communities.msn.com/content/features/photoalbum.asp
MSNSpaces
www.msnspaces.com
Myspace
www.myspace.com
Myyearbook
www.myyearbook.com
Picasa
http://picasa.google.com/index.html
Tribenetwork
www.tribenetwork.com
Wikipedia
http://en.wikipedia.org/wiki/Main_Page
Xanga
www.xanga.com
YouTube
www.youtube.com

Equity in Education

Equity issues are a major concern of educators who use technology in the classroom. Gender and equal availability of technology for everyone are the main issues (Siek et al., 2006). Research has documented that boys are more interested and involved with technology than are girls. Software generally tends to emphasize male-dominated activities. Games often include violence and competition as motivation. These software
Characteristics tend to attract males. Therefore, careful student software selection is essential for addressing gender in the classroom.

Student access to technology is dependent on the financial capabilities of a school or school district. Although student-to-computer ratios are steadily improving, many low socioeconomic schools have limited access to computers and the World Wide Web, especially classroom access. The Universal Service Fund for Schools and Libraries, referred to as the “E-Rate,” was created in 1996 to provide discounts on the cost of telecommunication services and equipment to public and private schools and libraries. The E-Rate program has connected more than a million classrooms to the Internet. Although Congress and state governments have taken steps to increase access through the E-Rate as well as other technology grant programs, the gap is still significant. A new type of poverty—information poverty—has emerged from this gap or digital divide.

Educators are concerned that information poverty will create a form of technological elitism. In a technologically oriented economy, people with more computer experience will obtain higher salaries, and people with little or no computer experience will be disadvantaged. The U.S. Department of Commerce (2004) documented the digital divide gap since 1994. Educators have a responsibility to ensure that all students have sufficient access to computers and the Internet, regardless of gender, ethnicity, socioeconomic background, and intellectual or physical ability.

Although the U.S. Department of Commerce (2000) documented slight increases in minority access to technology, people with disabilities are only half as likely (based on the national average) to have Internet access. Only 25 percent of the population without disabilities have never used a computer, while close to 60 percent of the population with disabilities have never used a computer. Only 20 percent of the people who are blind or vision impaired have Internet access. When selecting computer hardware and software applications for classroom use, educators need to evaluate the hardware and software to determine its accessibility by students with disabilities. Techniques for ensuring accessibility to a website are documented by the Web Access Initiative of the World Wide Web Consortium (www.w3.org/wai).

Vision-impaired students may use screen access software, which translates information on the screen into synthesized speech or Braille. If a site does not offer a text-only version, comprehension problems may occur when the screen access software reads the available text. For instance, when a graphic is a navigational element such as a button or arrow and the image label reads 009.gif or the button’s text is labeled “click,” the screen access software reads “009.gif or click.” Vision-impaired students may not understand the decontextualized text and become disoriented. Even with assistive computer technology installed for students with disabilities, Internet research is not possible with inaccessible web page design. The Center for Applied Special Technology (CAST) is a nonprofit organization dedicated to expanding educational opportunities for individuals with disabilities through the development and innovative uses of technology (see its website at www.cast.org/index.cfm). CAST developed a web-based program that identifies a website’s accessibility problems and suggests solutions. The Equal Access to Software and Information (EASI) website at www.rit.edu/~easi provides invaluable assistance.
resources for teachers using technology as a tool toward inclusion and curriculum integration for students with disabilities.

Teachers must take advantage of technology so all students can be involved in more than the drill-and-practice activities often common in lower socioeconomic schools. Teachers need to be aware of web designs that do not take cultural connotations and disabilities into consideration. Access to technology is more importantly about the effective use and careful integration of technology into the curriculum than simply providing access or the acquisition of hardware and software.

The Digital Divide

Kandel (2006) indicates that the canyon between technology have and have-nots haunts us, constantly reminding us that access to technology has been, and continues to be, unfair. How can we ensure adequate and equal access to technology? Two strategies are critical: funding and teacher professional development (Kuperstein & Gentile, 1998). Parent groups, fund-raising, industry partnerships, and careful budgeting in schools can help improve access to technology. Interest groups such as the National Coalition for Equity in Education (www.math.ucsb.edu/NCEE) disseminate information. Similarly, the Digital Divide Network (www.digitaldividenetwork.org) is an online resource connecting communities with resources needed to address the current inequalities. In addition, the Digital Equity Network (http://digitalequity.edreform.net) is an online service providing high-quality resources that help address the digital divide in the classroom and community. Ongoing professional development and technical assistance support teachers’ efforts to transform their practice. Teachers must strive to arrange equitable access and facilitate students’ use of technology that addresses their individual needs, including their cultural identity, and promotes interaction with the global community. Salpeter (2006) reported progress is being made in several digital divide issues, but the problem has not been solved.

One Laptop per Child Initiative

The MIT Media Lab (Negroponte, 2005) has developed a $100 laptop—a technology that could revolutionize how we educate the world’s children. The initiative is called One Laptop per Child, OLPC, and you can learn more about it at http://laptop.media.mit.edu. Nicholas Negroponte, co-founder of the MIT Media Lab, first announced the project in January 2005 at the World Economic Forum in Switzerland and debuted a prototype of the $100 laptop at the UN conference in Tunis. Negroponte believes that laptops are both a window into the world and a tool with which to think. Laptops promote independent interaction and exploration, and with them, children “learn learning.” The focus is to close the gap on the digital divide by providing millions of children around the world with a computer. A crank on the laptop will provide the two watts of power to run the computer and a Wi-Fi mesh network will provide the connectivity. The first public display of the laptop was July, 2006. Visit the Laptop initiative site at www.laptop.com for the latest progress reports. Also the laptop wiki has related information at: http://wiki.laptop.org/go/Home.
A University-Copyrighted Computer Software Policy

Have you ever "borrowed" a computer program from a friend or coworker? Are copyrighted computer programs currently installed on your home or office computer? If so, do you know whether those programs were borrowed or installed with the permission of the copyright owner? Federal copyright law gives the copyright owner the exclusive right to determine who can install or borrow copyrighted computer software. If you or an authorized university representative purchased software from a reputable vendor, then that purchase probably included the purchase of a license for the purchaser of the software.

Before you use, share, or distribute the software, you should understand the terms of the license. If the software was purchased off the shelf or prepackaged, then the packaging will include the license terms.

This method of disclosing the license terms is sometimes referred to as shrink wrap licensing, because the language often provides that by opening the (shrink wrap) packaging, the purchaser agrees to be bound by the terms of the license. If the software was developed or customized for a particular purpose, an underlying written agreement may contain the terms of the license. If university employees developed the software in the course of or as part of their employment, then the copyright in the software will belong to the University's Board of Regents.

This means that no one can distribute the software or license or allow others to use it without the express, written authorization of someone authorized to contract on behalf of the board. Agreement to license software created by university employees should be reviewed by the Technology Collaboration and Licensing Office or the Office of General Counsel.

If the university hired a consultant or independent contractor to develop the software, the agreement with the consultant or contractor either should assign ownership of the copyright in the resulting software to the university or should contain the license terms governing the use and distribution of the software. All agreements with third parties (including students) for the purchase, lease, creation, or adaptation of software or other copyrighted materials for use by the university should be reviewed by the purchasing and business services offices or the Office of General Counsel.

License terms may restrict the individuals or sites that are authorized to use the software. The term of the use, the purpose of the use, and the ability to distribute and copy the software may also be limited by license terms. The license may describe penalties for violation of its terms.

Unauthorized copying or distribution of software may also result in civil and criminal liability under federal and state laws. The university and the individuals involved in the unauthorized copying may be liable even if the software was copied for an educational or a nonprofit use.

(continued)
Software publishers have taken aggressive steps to protect against infringement of their copyrighted software. These steps may include an audit of university computers to search for software being used without authorization. The presence of unlicensed software may result in considerable liability for the university and for individuals involved in unauthorized copying. In other words, unless you are an authorized user, that "free" copy of a copyrighted software program may not be free at all.

Source: Adapted from a document prepared by the Arizona State University Office of General Counsel, 2001.

SUMMARY

We have only begun to experience the radical changes that computers will make on society as we know it. Computer scientists and sociologists differ in their estimates of our technological future: Some foresee a stark 1984-type world; others, Toffler (1981) among them, predict a bright future in which humans, aided by advanced technology, function with greater freedom than ever before. Who is right remains to be seen, but this much is certain: Computers are bound to change our lives and our society in dramatic and irrevocable ways.

Computer fraud and abuse take many forms: theft of money, goods, and identity; unlawful use of information stored in computers' memories; and unauthorized use of computer time. Hackers enter computer systems without authorization. Software piracy, which is the theft of computer programs, can cause software prices to increase. The computer virus is another major concern of computer security. The entry of a virus can destroy or damage records and shut down computers. Generally, viruses and spyware are difficult to detect, but vaccines and antispyware are available to overcome them. Spam, email scams and phishing are part of our daily emails. Education must provide awareness education for students. Social networking has become very popular. Parents, teachers, and schools must work to maintain safe use by students.

Computer crimes are on the increase partly because of the increasing number of computers in society. There are various methods of maintaining security in the computer room, primarily by limiting access to the room to authorized personnel. The password is the traditional method of controlling entry into a computer system and limiting access to records. Biometric technology is increasingly being used to maintain security. In addition, many organizations screen potential employees in the hiring process.

In addition to concerns for the security of organizations, there is concern for the rights of individuals. The Federal Privacy Act of 1974 was enacted to protect the confidentiality of files generated by federal government computers. Several state
governments have passed laws to further protect the average citizen from illegal use of computer information. Besides computer crime, the issue of change in the labor force is another major concern.

Teachers face new challenges in technology-based education. First, they must strive to provide equal access to computers for all students, regardless of gender, ethnicity, socioeconomic background, and ability. Second, they must promote computer ethics in their classrooms. They can do this by setting an example of ethical computer use and by using tools such as role playing and simulations to examine ethical questions. Educators and parents are concerned about student privacy and access to inappropriate sites. In addition, plagiarism concerns about student assignments utilizing the World Wide Web are becoming a major concern. Technology provides opportunities but also provides concerns to teachers and parents. All must work together to take advantage of this powerful tool!

**LET'S SEE WHAT YOU CAN DO!**

1. Discuss the gender-related differences in attitudes toward computers.
2. What are the dangers of technological elitism?
3. Describe recent cases of fraudulent uses of computers.
4. Describe the differences between COPPA and COPA.
5. Research violations of individual rights to privacy through unauthorized access to records.
6. What are your concerns about computer viruses and spyware and what are you doing to prevent loss or misuse of your data due to a virus or spyware?
7. Research the effects of low-income technology access.
8. Review a popular educational software package and check for male-dominated roles in the software.
9. Review the methods of blocking inappropriate websites for eliminating student access in schools.
10. Write and present to the class a report on the progress of the Negroponte S100 computer initiative to help eliminate the digital divide.
11. What steps can you take to stop plagiarism in your classroom?
12. What dangers do you foresee in new technology? Will new technology render life more impersonal or threaten our privacy?
13. Compare the privacy policy of Yahoo! at [www.yahoo.com](http://www.yahoo.com) to the privacy notice of Amazon at [www.amazon.com](http://www.amazon.com). (Look at the bottom of the main page for the link to privacy information.) Take note of the “cookies” and personal information sections.
14. What are schools and teachers main concerns with social networking?
15. Outline a plan to implement a Kid Safety program in your classroom.
16. List ten social networks and identify what safety requirements are in place to protect the user.
17. Identify all the states that have one-one computing initiatives. Describe each program.
18. Research the digital divide issues and write a summary of the progress, if any, that has been made to alleviate the problem since 2003.
19. List the copyright acts listed in this chapter which effect children. Develop a PowerPoint presentation for presentation to the PTA.
20. Research the effects of cybercrime on society.
**Computer Usage: Policies and Security**

This video clip provides additional information on the social, ethical, legal, and human issues teachers face when they incorporate technology into education.

- Log into [www.mylabschool.com](http://www.mylabschool.com), select Educational Technology under the Course tab, access the “Planning Technology-Enhanced Instruction” videos, and watch “Learning the Rules for Computer Use.”

  You may also navigate directly to the videos by entering Assignment ID ETV1 into the Assignment Finder.

Draft an acceptable use policy for your school.

---

**COMPANION WEBSITE**

To access chapter objectives, practice tests, weblinks, glossary, and flash cards, as well as the complete chapter bibliography, visit the companion website at [www.ablongman.com/bitter7e](http://www.ablongman.com/bitter7e).

---

![TECHNOLOGY IN THE CLASSROOM](image)