Chapter VII
Preparing Students for Ethical Use of Technology:
A Case Study for Distance Education

Deb Gearhart
Troy University, USA

ABSTRACT

Are our students prepared to use technology ethically? This is a question of concern to this author and addressed in this chapter. Experience as the director of a distance education program with students who are ill-prepared for using technology and who use technology unethically had lead to the research for this chapter. The chapter reviews studies where ethical behaviors are reviewed. The survey responses lead to discussion on how to instill ethical use of technology for institutional distance education programs, through the use of ethical policies and procedures. The chapter concludes with a look at future research directions.

INTRODUCTION

Kidder (1995) addressed the question "why should we teach ethics in an electronic age?" by responding that we will not survive the 21st century with the ethics of the 20th century. This is becoming more evident in our teaching practices. A U. S. Department of Justice report on the ethical use of information technology in education described what the authors term "psychological distance." When interacting with others face-to-face, the results of inappropriate and unethical behaviors are viewed immediately. When using information technology, inappropriate and unethical behavior while interacting with others can do harm. The act feels less personal because there is no immediate reaction in the exchange. The report goes on to note that traditionally moral values are learned at home and usually reinforced in school. That is not necessarily true today. Often values are not learned at home and schools are restricted in their ability to teach social values. In addition, young people are very comfortable with technology such as computer chats, instant messaging, text messaging, and so forth, where face-to-face interaction is not necessary. Our young people are becoming *psychologically distant* in their interactions with others.

As students move from school to the workplace, ethical issues for computing and information technology in education are becoming societal issues, dealing with both moral and criminal issues. Institutions of higher education need to deal with ethical issues related to computer technology. How do we teach and practice technology ethics in higher education? Here are two recommendations to be addressed in this chapter: set policy that provides a model for students to follow, and incorporate technology ethics issues in the curriculum. This chapter defines ethics and looks at how higher education, and in particular distance education, can deal with ethical issues encountered by students in using computing technology for educational purposes.

BACKGROUND

As early as 1990, informal polls showed that as many as three quarters of students on campuses today admit to some sort of academic fraud (Gearhart, 2000). Until recently research on ethics had been limited. There were two studies that demonstrated the need for a code of ethics in higher education. The first study was conducted in 1993 and a replicated study was conducted in 2001. In the first study 52.2% of education practitioners surveyed found a need for a code of ethics. When replicated in 2001, 72.8% of the education practitioners surveyed found a need for a code of ethics, demonstrating an increasing need for ethics in higher education (Brockett & Hiemstra, 2004, p. 10).

However, before dealing with educational ethics, a review of societal ethics is in order. In our society, quickly becoming a global society where information technology is concerned, the growing use of computers is becoming the norm in the workplace and in our daily lives. We are increasingly dependent on the computer.

Forester and Morrison (1994) looked at the social problems created by computers and have developed seven categories of computer-related ethical issues:

1. computer crimes and problems of computer security;
2. software theft and the question of intellectual property;
3. the problem of hacking and the creation of viruses;
4. computer unreliability and key questions on software quality;
5. data storage and invasion of privacy;
6. the social implications of artificial intelligence and expert systems; and
7. the many problems associated with workplace computerization.

All seven of these issues can be considered computer crime. Computer crime generally has been defined as a criminal act that has been committed using a computer as the principal tool. It takes the form of theft of money, theft of information, or theft of goods. These issues are not only moral and ethical issues, but can be very costly. Computer crime costs companies billions of dollars every year. Also, all seven of these issues can be found in higher education and have an effect on distance education.

DEFINING ETHICS

For the purposes of this chapter, ethics is defined as a three-tier process. In the first tier, ethics is simply the study of right and wrong, of good and evil, in human conduct. The second tier involves meta-ethics, the formal study of good and bad, or right and wrong, but not the real-life instances of such behavior. The third tier examines normative ethics, the choices people make and the values behind them, where the judgments about values in a particular moral issue are addressed (Brockett & Hiemstra, 2004, pp. 5-6).

In understanding the first tier, the basic principle of right and wrong, ethics has been defined as the code or set of principles by which people live. Ethics is about what is considered to be right and what is considered to be wrong. When people make ethical judgments, they are making prescriptive or normative statements about what ought to be done, not descriptive statements about what is being done (Forester & Morrison, 1994).

To describe the second tier, look at the question: What is ethical? Webster's Collegiate Dictionary defines ethics as "the discipline dealing with what is good and bad and with moral duty and obligation." More simply, it is the study of what is right to do in a given situation; what we ought to do. Alternatively, it is sometimes described as the study of what is good and how to achieve what is good. To suggest whether an act is right or wrong we need to agree on an ethical system that is easy to understand and apply. Spafford (1997) commented that a system of ethics that considers primarily only the results of our actions would not allow us to evaluate our current activities at the time when we would need such guidance. If we are unable to discern the appropriate course of action prior to its commission, then our system of ethics is of little or no values to us. To obtain ethical guidance, we must base our actions primarily on evaluations of the actions and not on the possible results. More to the point, if we attempt to judge the morality of an ethical action based on the sum total of all future effects, we would be unable to make such a judgment, either for a specific incident or for the general class of acts. In part, this is because it is so difficult to determine the long-term effects of various actions and to discern their causes. This ethical view is very important in teaching students about ethical behaviors with using technology. It is important

Table 1. Ethical principles for students and professionals

Honor	Is the action considered beyond reproach?
Honesty	Will the action violate any explicit or implicit trust?
Bias	Are there any external considerations that may bias the action to be taken?
Professional adequacy	Is the action within the limits of capability?
Due care	Is the action to be exposed the best possible quality assurance standards?
Fairness	Are all stakeholders' views considered with regard to the action?
Consideration of social cost	Is the appropriate accountability and responsibility accepted with respect to this action?
Effective and efficient action	Is the action suitable, given the objectives set, and is it to be completed using the least expenditure of resources?

Source: Rogerson, S., & Gotterbarn, D. (1998). The ethics of software project management. UK: Centre for Computing and Social Responsibility, De Montfort University.

for students to understand that inappropriate and criminal behaviors when using technology will have a profound effect on the future.

In the third tier, we look at the normative ethics of technology which affects distance education. In 1985, Moor defined computer ethics, which included computers and associated technology, as the analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology. Computing technology is essentially involved in every aspect of our lives. Technology-related ethics will not be something set in stone, nor will it be acceptable to state that all technology use is done to protect the whole of society. However, basic concepts of ethical behavior should be observed when using technology, whether it be for personal use, educational use or professional use. The Association of Computing Machinery (ACM) has developed a code of ethics for their organization (Appendix A) which deals with basic philosophies of doing no harm to others to the ethics related to their organization. Codes, such as this, are a good way to define how ethics works for a particular organization or practice.

In Table 1, Rogerson and Gotterbarn (1998) provide eight ethical principles for students and professionals.

In the example of an online course, these principles can be used to analyze and inform those working on the course as to whether ethical practices are being used. By considering which of the ethical principles apply to the course, it is possible to ascertain which activities within a course are ethically charged. Attention can then be paid to the ethical issues of the course.

SUPPORTING RESEARCH

Dakota State University (DSU) has recognized the need for ethical practices in higher education and has a mission driven response to ethical issues through an information technology literacy requirement for all students.

The information technology literacy requirements at DSU are intended to provide opportunities for students to develop additional skills in academic areas related to computer technology. At DSU, the information technology literacy requirements emphasize software applications and programming. The students will: 1) be knowledgeable and competent users of computer technology, and 2) use technology appropriately to understand processes and concepts in math and science and to solve problems in those disciplines (DSU Undergraduate Catalog 2005-2006, p. 79).

Table 2. 2003 NSSE experimental technology questions: Percent of students responding "very often" or "often" (One question excerpt)

	First-year DSU Students	First-year Students Peers	Seniors at DSU	Seniors Peers
How often do students at your institution copy and paste information from the WWW/Internet into reports/papers without citing the source?	47%	27%	55%	32%

Source: DSU Office of Institutional Effectiveness and Assessment

Incorporated in the information technology literacy requirement is the ethical use of technology and learning sound research techniques.

The Office of Institutional Effectiveness and Assessment provided information for the 2003 National Survey of Student Satisfaction (NSSE) conducted at DSU. This survey was given to freshman and seniors. Among the experimental technology questions asked in 2003 was "How often do students at your institution copy and paste information from the WWW/Internet into reports/papers without citing the source?" This question is one addressing students' ethical perspectives related to technology use. Table 2 shows the DSU freshmen and senior responses in relation to their peers nationally.

The DSU student responses are of concern when compared to the national norms. With one of the DSU general education requirements being in information literacy, the ethical issues of using materials from the Web should be addressed.

The Office of Institutional Effectiveness and Assessment provided the responses to the ethics question for the graduate survey and employer survey for 2003. Tables 3 and 4 represent those results.

Demonstrated by the survey results for the graduate and employer surveys, both responded

Table 3. 2003 graduate survey: Ability to use information ethically in your position

	Frequency	Percent	Cum Freq	Cum %
Very Satisfied	60	47.6	60	47.6
Satisfied	55	43.7	115	91.3
Neutral	10	7.9	125	99.2
Dissatisfied	1	0.8	126	100
Very Dissatisfied	0	0		
No Response	0	0		

Source: DSU Office of Institutional Effectiveness and Assessment

Table 4. 2003 employer survey: Ability to use information ethically

	Frequency	Percent	Cum Freq	Cum %
Very Good	34	49.3	34	49.3
Good	29	42.0	63	91.3
Fair	3	4.3	66	95.6
Poor	1	1.4	67	97.1
No Response	2	2.9	69	100

Source: DSU Office of Institutional Effectiveness and Assessment

Table 5. 2005 graduate survey: Ability to use information ethically in your position

	Frequency	Percent	Cum Freq	Cum %
Very Satisfied	45	42.9	45	42.9
Satisfied	52	49.5	97	92.4
Neutral	8	7.6	105	100
Dissatisfied	0	0		
Very Dissatisfied	0	0		
No Response	0	0		

Source: DSU Office of Institutional Effectiveness and Assessment

Table 6. 2005 employer survey: Ability to use information ethically

	Frequency	Percent	Cum Freq	Cum %
Very Good	37	52.1	37	52.1
Good	26	36.6	63	88.7
Fair	5	7.04	68	95.7
Poor	0	0	68	95.7
No Response	3	4.2	71	100

Source: DSU Office of Institutional Effectiveness and Assessment

that DSU graduates/new employees could use information ethically, 91.3% cumulatively.

The same questions were asked again in the 2005 Graduate and Employer Surveys. The results were similar, showing consistency over time.

92.4% of the graduates were satisfied or very satisfied with their ability to use information ethically and 88.7% of the employers rated the graduates' ability to use information ethically as good or very good.

If the questions on the NSSE survey are an indicator of the ethical judgments of students' use of technology then responding affirmatively to the graduate survey would present a discrepancy in ethical behaviors of the students and their perceptions of their own ethical behaviors. This presents an area to be further researched on the DSU campus. Do the DSU students understand what ethical behavior is, especially ethical behavior when using technology? Are the students also prepared with ethical research practices for the Internet?

This research, and questions addressed, was presented at a symposium on campus in the spring of 2005. The concern about ethical behavior was recognized as an issue the campus should address.

Each semester the campus conducts an academic convocation. In the fall of 2005 the theme of the convocation was ethics. The convocation was a kickoff to an online discussion for the remainder of the semester where both students and faculty participated. The campus continues to support the teaching of ethical behaviors in courses. This includes both campus and distance courses for the institutions.

Several studies conducted both in the K-12 setting and in higher education provide groundwork for the DSU study and provide data similar to that of the DSU study. Doherty and Orlofsky (2001) reported on a survey conducted with 500 students in grades 7-12. According to student response, 92% of students said having good computer skills improves the quality of people's lives "a great deal" or "somewhat, " but only 40% said that knowing about computers is "extremely" or "very " important to how well they do in school (p. 45). Also, the survey reported that 56% of the students felt they learned more about computers at home and that 61% noted their home computers were better than at school. In 2001, this survey noted that schools were probably not using technology as effectively as they could. Comments from this survey support the concept that students are not acquiring technology skills in high school, and come into higher education with a lack of formal training and understanding of the concepts needed for the use of technology, except what they learn in the home. This would include the lack of the ethical use of technology. It is the job of those in higher education to instill the ethical values of using technology and it is a difficult task when bad habits are learned early on, with the secondary education system not providing the training needed. Additional research in this area, with the survey of secondary students and teachers, may find this has improved since 2001.

Spain, Engle and Thompson (2005) discuss the frustrations business professors have when teaching ethics. Some professors feel that ethics cannot be taught. Others find it a challenge to instill ethical values in students or to have students understand the issues of social responsibility leading to ethical behavior. In the study presented by Spain, Engle and Thompson (2005), the university discussed conducted an event on its campus, similar to that of the DSU convocation, an "Ethics Awareness Week" (EAW). The EAW provided an opportunity:

1. for the faculty as a whole to focus on issues of ethics and social responsibility in their respective classes;
2. for students to have exposure to and articulation of ethics and social responsibility issues; and
3. for an interesting case study that the students can relate to which stimulated debate not only on the issues of ethics and social responsibility, but also how these issues related to particular majors/courses of study (p. 9).

The results of this project demonstrated that students' learning, related to ethics, can be influenced when a wide range of interdisciplinary teaching methods are used along with the EAW and the use of a debate. The main effects of the project upon enhanced student learning and understanding of ethical and social responsibility issues resulted from:

1. utilizing multiple pedagogical methods;
2. presentations by faculty from a variety of disciplines; and
3. the extended length of exposure to these discussions (p.14).

A study reported by McCabe, Trevino, and Butterfield (1999) further supported the instilling of ethical behaviors in students. The study reviewed surveys completed by 2310 students at colleges with both honor code and nonhonor code environments. There are three themes that became apparent from the study:

1. institutional/contextual factors related to academic integrity;
2. attitudes/personal factors related to academic integrity; and
3. institutional/contextual factors related to academic dishonesty (pp.215-216).

The first theme of the study was that in institutions with honor codes there are lower levels of academic dishonesty because the expectations are clearly spelled out in the code. Students confirmed that in their responses. Although not a question asked directly because the students in nonhonor code institutions would not have a code to respond to, academic integrity was spelled out in the open-ended responses of the students. Students in the honor code institutions commented that there was more of an effect by faculty and administrators to help prevent cheating.

There were varying attitudes toward cheating described by the students participating in the survey, the second theme. In both the honor code and nonhonor code institutions, the justifications for why students cheat ranged from family pressures, societal expectations, pressure for grades, and graduate school to laziness and apathy. Many students described "grey areas" where there were no expectations or definition of cheating, especially for assignments. The third theme of institutional factors related to academic dishonesty addressed how the students participating in the survey described the ineffectiveness of institutional policies on actual cheating within the institution and on how the pressure to report other cheating students affected students. It was clear that many of the students participating in the survey felt the institutional honor codes were ineffective and that students were uncomfortable in reporting fellow students.

Like the survey of high school students, this study, conducted prior to the DSU research, provides valuable insight to students' understanding of the issues of cheating. One student commented that society expects students to cheat; a sad statement to what higher education faces when dealing with students entering its prevue. As this chapter is dealing specifically with ethical use of technology, it becomes apparent that institutions must address policy related to the technology use on campus and for all aspects of the institution. Most policy or procedure manuals deal with technical requirements needed to support the learning experience. However, computing privilege policies are quickly addressing inappropriate behaviors and ethical issues. It has become apparent from the studies described in this section that this issue must be dealt with by the entire institution and not just in specific program areas, such as business or medical programs. When looking at the institution as a whole, distance programs are as much a part of this issue as any other area of the institution. Although distance programs are very aware of quality assurance issues within programs, the dealing of ethics for distance learners is an area which still needs to be clearly defined.

ETHICAL ISSUES RELATED TO DISTANCE EDUCATION

The E-learning Program staff at DSU has worked with faculty to deal with ethical issues in distance courses, particularly with cheating. This section of the chapter will address ethical issues related to distance course delivery and computer usage by students. Student behaviors and policy issues related to these behaviors are also discussed.

It is important to understand what leads to ethical dilemmas for students, such as cheating. As pointed out in the studies described in the pervious section, pressure for good grades, the testing environment, the lack of understanding of academic regulations, personality characteristics, and development of moral reasoning all can lead to cheating. Fass (1990) commented that many colleges and universities do not adequately spell out information on cheating in their handbooks and catalogs, which is still an issue today. Students coming from high school do not understand the issues of collegiate ethics and academic honesty. Fass recommends that the following areas should be addressed in university handbooks and be provided to both the traditional and distance student.

- Ethics of examinations
- Use of sources on papers and projects
- Writing assistance and other tutoring
- Collecting and reporting data
- Use of academic resources
- Respecting the work of others
- Computer ethics
- Giving assistance to others
- Adherence to academic regulations (pp. 173-173).

Terms that should be spelled out in policies related to computer technology include the following; however, this is not an all inclusive list.

- **Copy Protection:** A method originated by software developers to prevent a disk from being copied.
- **Copyright:** The legal right granted to an author, computer user, playwright, publisher, or distributor to exclusive publication, production, sale, or distribution of a literary, musical, dramatic, or artistic work.
- **Ethics:** A system of moral principles.
- *Freeware.* Software programs–usually written for fun by a hobbyist–offered for use free of charge.
- **Legal:** Permitted by law.
- **License:** An agreement between the vendor and the purchaser of software.
- **Piracy:** The copying or duplicating of computer software without proper authorization.
- **Public domain software:** Software available to anyone at no cost, or at a limited cost to cover the expense of the disk and the copying service.
- **Shareware:** Software available for free trial use. If users like the product, they are requested to submit a registration fee.
- **Softlifing:** The process of making illegal copies for personal use or for friends.

Review your institution's policies, both for applicability to distance education and to determine if the policies are ethically sound. It is important for a distance education program to develop a set of policies that represent the campus policy with the adaptation, if necessary, for the distance student. Create new policies when there are no current policies. Keep in mind the diverse populations encountered in distance education. Then, make the policies accessible to your distance students and keep them updated. Make sure that all campus services are provided to your distance students and again make sure they know about them.

Work with the faculty to explain how they can assist in developing an ethically sound distance learning atmosphere. Providing information to the learners, in multiple formats, is critical. Information must be addressed in the syllabi; course Web sites, assignments, examinations and projects with the deadlines; discussion boards' instructions, including "netiquette" used, and the information the instructor provides on plagiarism and cheating, instructor availability, assignment submission, learner support for technical issues and other learner support. Reinforce this, as once is not enough, especially as Web courses are "living" entities, always changing. Instructors must keep their learners informed of changes made during the course.

Work with your faculty on developing and improving e-learning policies. Faculty members work firsthand with the learners and see what works and what doesn't. The online faculty members at DSU meet regularly throughout the semester and have worked as a group to implement new policy relevant to our e-learning program.

Finally, when it comes to policy, the work is never finished, especially when related to constantly changing technology. Keeping policy ethical and current is a never ending process. Use the institutional course assessment procedure as the guide to implementing changes to the distance education program, reviewing your policies at the same time.

The following information is an example of policy or procedures that can be provided on creation of passwords for distance students to help avoid hacking. Boob (2006) provides five tips for passwords to help avoid hacking: 1) No password should be permitted that contains all or part of the user's name, ID number, or some easily guessed element; 2) Every password must use a variety of kinds of symbols and keys; 3) However, passwords should be immune to dictionary-based hacking attacks yet can be remembered by the user (e.g., 4Whippet meets this but pW4hIpt?e, does not); 4) Theoretically, changing passwords frequently is considered good security, however, users forget passwords easily and write them down, so set password change intervals at 90 days and education users on security and password creation; and finally 5) Longer is better; passwords that are 15 characters or longer are treated as essentially unhackable.

CONCLUSION

How will the ethics of distance education look in the future? Two scholars in the field of ethics have developed theories. Gorniak-Kocikowska suggests that computer technology-based ethics will evolve into an overarching, global view of ethics for the information age. The view taken by Johnson is similar. As information technology becomes commonplace and is integrated into everyday life, so does technology-based ethics become part of ordinary ethics (Bynum, 2001). In education we see the term "distance" disappearing from distance education; it is just education delivered in many formats. We will also see technology-based ethics become ethics for our society and not specifically geared to a discipline.

FUTURE RESEARCH DIRECTIONS

There are two research directions for further study of this topic. The DSU study was based on survey questions completed by students on a regular basis but with only limited information on ethics. A survey designed specifically addressing the issues related to ethical use of technology should be administered. Such a survey then could be replicated at other institutions to validate the survey and the findings. The second area of research would involve the development of ethical policy and procedures at the institutional level and a review conducted over time to ascertain if the policies or procedures made a difference in student behavior in the ethical use of technology. As an area of research, the ethical use of technology can provide a future research direction for some time.

REFERENCES

Boob, V. (2006). People, problems, and passwords. *IT Trends, 66,* 8-10.

Brockett, R. G. & Hiemstra, R. (2004). *Toward ethical practice*. Malabar, FL: Krieger Publishing Company

Bynum, T. (2001, Winter). Computer ethics: Basic concepts and historical overview. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy.* Retrieved April 16, 2008, from http://plato.stanford.edu/archives/win2001/entries/ethics-computer

Doherty, K. M., & Orlofsky, G. F. (2001). Student survey says: Schools are probably not using educational technology as wisely or effectively as they could. *Education Week, 20*(35), 45-48.

DSU Undergraduate Catalog 2005-2006. Retrieved on January 20, 2005, from http://www.departments.dsu.edu/registrar/catalog/PDF/2005-06undergraduate.pdf

Fass, R. A. (1990). Cheating and plagiarism. In W. May (Ed.), *Ethics and higher education.* New York: Macmillan Publishing Company and American Council on Education.

Forester, T., & Morrison, P. (1994). *Computer ethics, cautionary tales and ethical dilemmas in computing* (2nd ed.). Cambridge, MA: The MIT Press.

Gearhart, D. (2000). Ethics in distance education: Developing ethical policies. *The Online Journal of Distance Learning Administration, 4*(1). Retrieved April 16, 2008, from Http://www.westga.edu/~distance/ojdla/spring41/gearhart41.html

Kidder, R. M. (1995). The ethics of teaching and the teaching of ethics. In E. Boschmann (Ed.), *The electronic classroom: A handbook for education in the electronic environment.* Medford, NJ: Learned Information.

McCabe, D. L., Trevino, L. K., & Butterfield, K. D. (1999). Academic integrity in honor code and non-honor code environments: A qualitative investigation. *The Journal of Higher Education, 70*(2), 211-234.

Moor, J. H. (1985). What is computer ethics? *Metaphilosophy, 16*(4), 266-275.

Rogerson, S., & Gotterbarn, D. (1998). *The ethics of software project management.* Centre for Computing and Social Responsibility, De Montfort University, UK. Retrieved April 16, 2008, from http://ccsr.cse.dmu.ac.uk/staff/Srog/teaching/sweden.htm

Spafford, E. H. (1997). Are hacker break-ins ethical? In M. D. Ermann, M. B. Williams, & M. S. Shauf (Eds.), *Computers, ethics, and society.* New York: Oxford University Press.

Spain, J. W., Engle, A. D., & Thompson, J. C. (2005). Applying multiple pedagogical methodologies in an ethics awareness week: Expectations, events, evaluation, and enhancements. *Journal of Business Ethics, 58,* 7-16.

ADDITIONAL READINGS

Allen, J., Fuller, D., & Luckett, M. (1998). Academic integrity: Behaviors, rates, and attitudes of business students toward cheating. *Journal of Marketing Education*, *20*(1), 41-52.

Association for Computing Machinery (ACM). (1992). ACM proposed code of ethics and professional conduct. *Communications of the ACM, 35*(5), 94-99.

Bayles, M. D. (1981). *Professional ethics.* Belmont, CA: Wadsworth.

Blatt, M., & Kohlberg, L. (1975). The effects of classroom moral discussion on children's level of moral development. *Journal of Moral Education*, 4.

Bynum, T. W. (Ed.). (l985, October). *Computers & Ethics, 6*(4). Basil Blackwell.

Bynum, T. W., Maner, W., & Fodor, J. (Eds.). (1992). *Teaching computer ethics*. New Haven: Southern Connecticut State University, Research Center on Computing and Society.

Cizek, G. (1999). *Cheating on tests: How to do it, detect it, and prevent it*. Mahwah, NJ: Lawrence Erlbaum.

Collins, W. R., & Miller, K. W. (1992, January). Paramedic ethics for computer professionals. *Journal of Systems and Software, 17*, 23-38.

Crown, D., & Spiller, M. (1998). Learning from the literature on collegiate cheating: A review of empirical research. *Journal of Business Ethics, 17*, 683-700.

DeGeorge, R. (1990). *Business ethics* (3rd ed.). New York: Macmillan.

Dunlop, C., & Kling, R. (Eds.). (l991). *Computerization & controversy: Value conflicts & social choices*. Academic Press.

Ellenberg, J. H. (1983). Ethical guidelines for statistical practice: A historical perspective. *The American Statistician, 37*(1), 1-13.

Erdmann, M. D., Willimas, M. B., & Gutierrez, C. (l990). *Computers, ethics and society*. Oxford University Press.

Evans, E. D., Craig, D., & Mietzel, G. (1993). Adolescents' cognitions and attributions for academic cheating: A cross-national study. *The Journal of Psychology, 127*(6), 585-602.

Forester, T., & Morrison, P. (l990). *Computer ethics: Cautionary tales and ethical dilemmas in computing*. The MIT Press.

Frankel, M. S. (1989). Professional codes: Why, how, and with what impact? *Journal of Business Ethics, 8*(2 & 3), 109-116.

Franklyn-Stokes, A., & Newstead, S. E. (1995). Undergraduate cheating: Who does what and why? *Studies in Higher Education, 20*(2), 159-72.

Gotterbarn, D. (1991, Summer). Computer ethics: Responsibility regained. *National Forum,* 26-32.

Gotterbarn, D. (1992, August). Ethics and the computing professional. *Collegiate Microcomputer, 10*(3).

Gould, C. (l989). *The information Web: Ethical and social implications of computer networking*. Westview Press.

Hall, R. T., & Davis, J. U. (1975). *Moral education in theory and practice*. Prometheus Books.

Heberling, M. (2002). Maintaining academic integrity in online education. *Online Journal of Distance Learning Administration, 5*(2). Retrieved April 16, 2008, from http://www.westga.edu/%7Edistance/ojdla/spring51/spring51.html

Hinman, L. M. (2000, November 2). *Academic integrity and the World Wide Web*. Retrieved April 16, 2008, from http://ethics.acusd.edu/presentations/cai2000/index_files/frame.htm

Illinois Online Network. (2001). *Strategies to minimize cheating online*. Retrieved April 16, 2008, from http://illinois.online.uillinois.edu/pointer/IONresources/assessment /cheating.html

Johnson, D. W. (l984). *Computer ethics: A guide for the new age*. Brethren Press.

Johnson, D. G. (1985). *Computer ethics*. Prentice Hall.

Johnson, D. G. (1991). *Ethical issues in engineering*. Englewood Cliffs, NJ: Prentice Hall.

Johnson, D. G. (1993). *Computer ethics* (2nd ed.). Englewood Cliffs, NJ: Prentice Hall.

Johnson, D. G., & Snapper, J. W. (Eds.). (1985). *Ethical issues in the use of computers*. Belmont, CA: Wadsworth.

Kleiner, C., & Lord, M. (1999). The cheating game: Cross-national exploration of business students' attitudes, perceptions, and tendencies toward academic dishonesty. *Journal of Education for Business, 74*(4), 38-42.

Lambert, K., Ellen, N., & Taylor, L. (2003). Cheating ? What is it and why do it: A study in New Zealand tertiary institutions of the perceptions and justification for academic dishonesty. *Journal of American Academy of Business, 3*(1/2), 98-103.

Lee, C. (1986, March). Ethics training: Facing the tough questions. *Training*, 30-41.

Lim, V. K. G., & See, S. K. B. (2001). Attitudes toward, and intentions to report, academic cheating among students in Singapore. *Ethics and Behavior, 11*(3), 261-74.

Martin, C. D., & Martin, D. H. (1990). Comparison of ethics codes of computer professionals. *Social Science Computer Review, 9*(1), 96-108.

Martin, M. W., & Schinzinger, R. (1989). *Ethics in engineering*. McGraw-Hill.

McCabe, D. L., & Trevino, L. (1995). Cheating among business students: A challenge for business leaders and educators. *Journal of Management Education, 19*(2), 205-18.

McCabe, D. L., & Trevino, L. K. (1996). What we know about cheating in college. *Change, 28*(1), 29-33.

McMurtry, K. (2001). E-cheating: Combating a 21st century challenge. *The Journal Online: Technological Horizons in Education*. Retrieved April 16, 2008, from http://thejournal.com/magazine/vault/A3724.cfm

O'Neill, P., & Hern, R. (1991). A systems approach to ethical problems. *Ethics & Behavior, 1*, 129-143.

Parker, D. B. (1979). *Ethical conflicts in computer science and technology*. Arlington, VA: AFIPS Press.

Parker, D. B., Swope, S., & Baker, B. N. (1991). *Ethical conflicts in information and computer science, technology, and business*. QED Information Sciences.

Phillips, M. R., & Horton, V. (2000). Cybercheating: Has morality evaporated in business education? *The International Journal of Educational Management, 14*(4), 150-5.

Roberts, D. M., & Rabinowitz, W. (1992). An investigation of student perceptions of cheating in academic situations. *The Review of Higher Education, 15*(2), 179-90.

Robinett, J. (Ed.). (l989). *Computers & ethics: A sourcebook for discussions*. Polytechnic Press.

Schlaefi, A., Rest, J. R., & Thoma, S. J. (1985). Does moral education improve moral judgment? A meta-analysis of intervention studies using the defining issues test. *Review of Educational Research, 55*, 319-52.

Sivin, J. P., & Bialo, E. R. (1992). *Ethical use of information technologies in education: Important issues for America's schools.* Washington, DC: National Institute of Justice. Stevenson, J. T. (1987). *Engineering ethics: Practices and principles*. Toronto: Canadian Scholars Press.

Thompson, L. C., & Williams, P. G. (1995). But I changed three words! Plagiarism in the ESL classroom. *Clearing House, 69*(1), 27-9.

Tom, G., & Borin, N. (1988). Cheating in academe. *Journal of Education for Business*, *63*(4), 153-7.

Underwood, J., & Szabo, A. (2003). Academic offences and e-learning: Individual propensities in cheating. *British Journal of Educational Technology, 34*(4), 467-77.

Valasquez, M. G. (1990). Corporate ethics: Losing it, having it, getting it. In P. Madsen & J. M. Shafritz (Eds.), *Essentials of business ethics* (pp. 228-244). Penguin Books.

Waugh, R. F., Godfrey, J. R., Evans, E. D., & Craig, D. (1995). Measuring students' perceptions about cheating in six countries. *Australian Journal of Psychology, 47*(2), 73-82.

APPENDIX A: ACM CODE OF ETHICS AND PROFESSIONAL CONDUCT

On October 16, 1992, ACM's Executive Council voted to adopt a revised Code of Ethics. The following imperatives and explanatory guidelines were proposed to supplement the code as contained in the new ACM Bylaw 17.

Commitment to ethical professional conduct is expected of every voting, associate, and student member of ACM. This code, consisting of 24 imperatives, formulated as statements of personal responsibility, identifies the elements of such a commitment.

It contains many, but not all, issues professionals are likely to face. Section 1 outlines fundamental ethical considerations, while Section 2 addresses additional, more specific considerations of professional conduct. Statements in Section 3 pertain more specifically to individuals who have a leadership role, whether in the workplace or in a volunteer capacity, for example, with organizations such as ACM. Principles involving compliance with this code are given in Section 4.

The code is supplemented by a set of guidelines, which provide explanation to assist members in dealing with the various issues contained in the code. It is expected that the guidelines will be changed more frequently than the code.

The code and its supplemented guidelines are intended to serve as a basis for ethical decision making in the conduct of professional work. Secondarily, they may serve as a basis for judging the merit of a formal complaint pertaining to violation of professional ethical standards.

It should be noted that although computing is not mentioned in the moral imperatives section, the code is concerned with how these fundamental imperatives apply to one's conduct as a computing professional. These imperatives are expressed in a general form to emphasize that ethical principles which apply to computer ethics are derived from more general ethical principles.

It is understood that some words and phrases in a code of ethics are subject to varying interpretations, and that any ethical principle may conflict with other ethical principles in specific situations. Questions related to ethical conflicts can best be answered by thoughtful consideration of fundamental principles, rather than reliance on detailed regulations.

1. **General Moral Imperatives. As an ACM member I will…**
   - **Contribute to society and human well-being**. This principle concerning the quality of life of all people affirms an obligation to protect fundamental human rights and to respect the diversity of all cultures. An essential aim of computing professionals is to minimize negative consequences of computing systems, including threats to health and safety. When designing or complementing systems, computing professionals must attempt to ensure that the products of their efforts will be used in socially responsible ways, will meet social needs, and will avoid harmful effects to health and welfare.

     In addition to a safe social environment, human well-being includes a safe natural environment. Therefore, computing professionals who design and develop systems must be alert to, and make others aware of, any potential damage to the local or global environment.
   - **Avoid harm to others**. "Harm" means injury or negative consequences, such as undesirable loss of information, loss of property, property damage, or unwanted environmental impacts. This principle prohibits use of computing technology in ways that result in harm to any of the following: users, the general public, employees, and employers. Harmful actions include intentional destruction or modification of files and programs leading to serious loss of re-

sources or unnecessary expenditure of human resources such as the time and effort required to purge systems of computer viruses.

Well-intended actions, including those that accomplish assigned duties, may lead to harm unexpectedly. In such an event the responsible person or persons are obligated to undo or mitigate the negative consequences as much as possible. One way to avoid unintentional harm is to carefully consider potential impacts on all those affected by decisions made during design and implementation.

To minimize the possibility of indirectly harming others, computing professionals must minimize malfunctions by following generally accepted standards for system design and testing. Furthermore, it is often necessary to assess the social consequences of systems to project the likelihood of any serious harm to others. If systems features are misrepresented to users, coworkers, or supervisors, the individual computing professional is responsible for any resulting injury.

In the work environment the computing professional has the additional obligation to report any signs of system dangers that might result in serious personal or social damage. If one's superiors do not act to curtail or mitigate such dangers, it may be necessary to "blow the whistle" to help correct the problem or reduce the risk. However, capricious or misguided reporting of violations can, itself, be harmful. Before reporting violations, all relevant aspects of the incident must be thoroughly assessed. In particular, the assessment of risk and responsibility must be credible. It is suggested that advice be sought from other computing professionals (See principle 2.5 regarding thorough evaluations).

- **Be honest and trustworthy**. Honesty is an essential component of trust. Without trust an organization cannot function effectively. The honest computing professional will not make deliberately false or deceptive claims about a system or design, but will instead provide full disclosure of all pertinent system limitations and problems.

  A computer professional has a duty to be honest about his or her own qualifications, and about any circumstances that might lead to conflicts of interest.

  Membership in volunteer organizations such as ACM may at times place individuals in situations where their statements or actions could be interpreted as carrying the "weight" of a larger group of professionals. An ACM member will exercise care not to misinterpret ACM or positions and policies of ACM or any ACM units.

- **Be fair and take actions not to discriminate**. The values of equality, tolerance, respect for others, and the principles of equal justice govern this imperative. Discrimination on the basis of race, sex, religion, age, disability, national origin, or other such factors is an explicit violation of ACM policy and will not be tolerated.

  Inequities between different groups of people may result form the use or misuse of information and technology. In a fair society, all individuals would have equal opportunity to participate in, or benefit from, the use of computer resources regardless of race, sex, religion, age, disability, national origin, or other such similar factors. However, these ideals do not justify unauthorized use of computer resources, nor do they provide an adequate basis for violation of any other ethical imperatives of this code.

- **Honor property rights including copyrights and patents**. Violation of copyrights, patents, trade secrets and the terms of license agreements is prohibited by law in most circumstances. Even when software is not so protected, such violations are contrary to professional behavior.

Copies of software should be made only with proper authorization. Unauthorized duplication of materials must not be condoned.

- **Give proper credit for intellectual property**. Computing professionals are obligated to protect the integrity of intellectual property. Specifically, one must not take credit for other's ideas or work, even in cases where the work has not been explicitly protected, for example, by copyright or patent.
- **Respect the privacy of others**. Computing and communication technology enables the collection and exchange of personal information on a scale unprecedented in the history of civilization. Thus, there is increased potential for violating the privacy of individuals and groups. It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals. This includes taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals. Furthermore, procedures must be established to allow individuals to review their records and correct inaccuracies.

  This imperative implies that only the necessary amount of personal information be collected in a system, that retention and disposal periods for that information be clearly defined and enforced, and that personal information gathered for a specific purpose not be used for other purposes without consent of the individual(s). These principles apply to electronic communications, including electronic mail, and prohibit procedures that capture or monitor electronic user data, including messages, without the permission of users or *bona fide* authorization related to system operation and maintenance. User data observed during the normal duties of system operation and maintenance must be treated with strictest confidentiality, except in cases where it is evidence for the violation of law, organizational regulations, or this code. In these cases, the nature or contents of that information must be disclosed only to proper authorities (See 1.8).
- **Honor confidentiality**. The principle of honesty extends to issues of confidentiality of information whenever one has made an explicit promise to honor confidentiality or, implicitly, when private information not directly related to the performance of one's duties becomes available. The ethical concern is to respect all obligations of confidentiality to employers, clients, and users unless discharged from such obligations by requirements of the law or other principles of this code.

2. **More Specific Professional Responsibilities. As an ACM computing professional I will…**
   - **Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work**. Excellence is perhaps the most important obligation of a professional. The computing professional must strive to achieve quality and to be cognizant of the serious negative consequences that may result from poor quality in a system.
   - **Acquire and maintain professional competence**. Excellence depends on individuals who take responsibility for acquiring and maintaining professional competence. A professional must participate in setting standards for appropriate levels of competence, and strive to achieve those standards. Upgrading technical knowledge and competence can be achieved in several ways: doing independent study; attending seminars, conferences, or courses; and being involved in professional organizations.

- **Know and respect existing laws pertaining to professional work**. ACM members must obey existing local, state, province, national and international laws unless there is a compelling ethical basis not to do so. Policies and procedures of the organizations in which one participates must also be obeyed. But compliance must be balanced with the recognition that sometimes existing laws and rules may be immoral or inappropriate and, therefore, must be challenged.

  Violation of a law or regulation may be ethical when that law or rule has inadequate moral basis or when it conflicts with another law judged to be more important. If one decides to violate a law or rule because it is viewed as unethical or for any other reason, one must fully accept responsibility for one's actions and for the consequences.
- **Accept and provide appropriate professional review**. Quality professional work, especially in the computing profession, depends on professional reviewing and critiquing. Whenever appropriate, individual members should seek and utilize peer review as well as provide critical review of the work of others.
- **Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks**. Computer professionals must strive to be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives. Computer professionals are in a position of special trust, and therefore have a special responsibility to provide objective, credible evaluations to employers, clients, users, and the public. When providing evaluations the professional must also identify any relevant conflicts of interest, as stated in imperative 1.3.

  As noted in the discussion of principle 1.2 on avoiding harm, any signs of danger from systems must be reported to those who have opportunity or responsibility to resolve them. See the guidelines for imperative 1.2 for more details concerning harm, including the reporting of professional violations.
- **Honor contracts, agreements, and assigned responsibilities**. Honoring one's commitments is a matter of integrity and honesty. For the computer professional this includes ensuring that system elements perform as intended. Also, when one contracts for work with another party, one has an obligation to keep that party properly informed about progress toward completing that work.

  A computing professional has a responsibility to request a change of assignment that he or she feels cannot be completed as defined. Only after serious consideration and with full disclosure of risks and concerns to the employer or client should one accept the assignment. The major underlying principle here is the obligation to accept personal accountability for professional work. On some occasions other ethical principles may take greater priority.

  A judgment that a specific assignment should not be performed may not be accepted. Having clearly identified one's concerns and reasons for that judgment, but failing to procure a change in that assignment, one may yet be obligated, by contract or by law, to proceed as directed. The computing professional's ethical judgment should be the final guide in deciding whether or not to proceed. Regardless of the decision, one must accept the responsibility for the consequences. However, performing assignments "against one's own judgment" does not relieve the professional of responsibility for any negative consequences.
- **Improve public understanding of computing and its consequences**. Computing professionals have a responsibility to share technical knowledge with the public by encouraging

understanding of computing, including the impacts of computer systems and their limitation. This imperative implies an obligation to counter any false views related to computing.

- **Access computing and communication resources only when authorized to do so**. Theft or destruction of tangible and electronic property is prohibited by imperative 1.2 – "Avoid harm to others." Trespassing and unauthorized use of a computer or communication system is addressed by this imperative. Trespassing includes accessing communication networks and computer systems, or accounts or files associated with those systems, without explicit authorization to do so. Individuals and organizations have the right to restrict access to their systems so long as they do not violate the discrimination principle (see 1.4).
  No one should enter or use another's computing system, software, or data files without permission. One must always have appropriate approval before using system resources, including .rm57 communication ports, file space, other system peripherals, and computer time.

3. **Organizational Leadership Imperatives. As an ACM member and an organizational leader, I will…**
   - **Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities**. Because organizations of all kinds have impacts on the public, they must accept responsibilities to society. Organizational procedures and attitudes oriented toward quality and the welfare of society will reduce harm to members of the public, thereby serving public interest and fulfilling social responsibility. Therefore, organizational leaders must encourage full participation in meeting social responsibilities as well as quality performance.
   - **Manage personnel and resources to design and build information systems that enhance the quality of working life**. Organizational leaders are responsible for ensuring that computer systems enhance, not degrade, the quality of life. When implementing a computer system, organizations must consider the personal and professional development, physical safety, and human dignity of all workers. Appropriate human-computer ergonomic standards should be considered in system design and in the workplace.
   - **Acknowledge and support proper and authorized uses of an organization's computing and communications resources**. Because computer systems can become tools to harm as well as to benefit an organization, the leadership has the responsibility to clearly define appropriate and inappropriate uses of organizational computing resources. While the number and scope of such rules should be minimal, they should be fully enforced when established.
   - **Ensure that users and those who will be affected by a system have their needs clearly articulated during the assessment and design of requirements. Later the system must be validated to meet requirements**. Current system users, potential users and other persons who lives may be affected by a system must have their needs assessed and incorporated in the statement of requirements. System validation should ensure compliance with those requirements.
   - **Articulate and support policies that protect the dignity of users and others affected by a computing system**. Designing or implementing systems that deliberately or inadvertently demean individuals or groups is ethically unacceptable. Computer professionals who are in decision-making positions should verify that systems are designed and implemented to protect personal privacy and enhance personal dignity.

- **Create opportunities for members of the organization to learn the principles and limitations of computer systems**. This complements the imperative on public understanding (2.7). Educational opportunities are essential to facilitate optimal participation of all organizational members. Opportunities must be available to all members to help them improve their knowledge skills in computing, including courses that familiarize them with the consequences and limitations of particular types of systems. In particular, professionals must be made aware of the dangers of building systems around oversimplified models, the improbability of anticipating and designing for every possible operating condition, and other issues related to the complexity of this profession.

4. **Compliance with the Code. As an ACM member I will…**
   - **Uphold and promote the principles of this code**. The future of the computing profession depends on both technical and ethical excellence. Not only is it important for ACM computing professionals to adhere to the principles expressed in this code, each member should encourage and support adherence by other members.
   - **Treat violations of this code as inconsistent with membership in the ACM**. Adherence of professionals to a code of ethics is largely a voluntary matter. However, if a member does not follow this code by engaging in gross misconduct, membership in ACM may be terminated.

ACM stands for Association of Computing Machinery.

Source: Forester, T., & Morrison, P. (1994). *Computer ethics cautionary tales and ethical dilemmas in computing* (2nd ed., pp. 261-270). Cambridge, MA: The MIT Press.