DOCUMENT RESUME

ED 374 780 IR 016 824

AUTHOR Brown, Lisa; And Others
TITLE Developing a Campus-Wide Computer Ethics Policy.
PUB DATE [Jun 94]
NOTE 12p.
PUB TYPE Reports - Descriptive (141)

EDRS PRICE MF01/PC01 Plus Postage.
DESCRIPTORS *Computer Networks; *Computer Uses in Education; *Ethics; Futures (of Society); Higher Education; *Policy Formation; *School Policy; Technological Advancement
IDENTIFIERS *Academic Computing; *Computer Ethics; Illinois Wesleyan University

ABSTRACT

This paper discusses the process for developing a campus-wide computer ethics policy at Illinois Wesleyan University. As a part of a campus-wide computerization planning effort, the university realized it would be necessary to set in place rules of conduct, methods of monitoring conduct, and penalties for transgressions of these policies. The need for a policy arose from the realization of problems relating to network integrity, liability, and software copyrights. A task force consisting of faculty and administration created a smaller group charged with developing the policy. The policy created focuses on legal and ethical issues of campus computing. Issues encountered while developing the policy include: whether or not to allow the use of games; the use of computer equipment for monetary gain; and academic dishonesty. An implementation plan was developed along with the policy: (1) obtain approval from the trustees; (2) include the policy in the faculty and student handbooks; and (3) mak students aware of the policy. The policy was adopted in April 1993 by the Board of Trustees of the university. Sections of the campus-wide ethics policy are interspersed with narrative in the paper describing the policy's development. (JLB)

Developing a Campus-wide Computer Ethics Policy

by Lisa Brown
L. W. Colter
Trey Short

Developing a Campus-wide Computer Ethics Policy

by Lisa Brown, L. W. Colter, and Trey Short
Illinois Wesleyan University

Introduction

As part of a campus-wide computerization planning effort, Illinois Wesleyan University realized it would be necessary to set in place rules of conduct, methods of monitoring conduct, and penalties for transgressions of these policies. Areas of particular concern were: the protection of academic freedom and privacy for faculty, compliance with software license agreements, and the problems associated with a campus dependent on distributed processing and desktop computing. The policy was developed by a faculty task-force and approved by the administration without revision. The present paper discusses the process for developing the policy and the means for implementation.

Background

Illinois Wesleyan University is a small, liberal arts university located in central Illinois. The University serves an undergraduate population of approximately 1800 students in the College of Liberal Arts and the Schools of Fine Arts, Music, Nursing, and Theatre Arts. The Carnegie Foundation reclassified Illinois Wesleyan recently from a Regional Comprehensive II to a Liberal Arts Baccalaureate I institution, largely on the basis of significant increases in the quality of the institution.

The Board of Trustees heads the University's structure. It is governed daily by its President, Provost/Dean of Faculty, and Associate Dean. Faculty committees relevant to campus computing include the Council on Policies and Procedures (CUPP - a campus-wide, representational committee). In addition, the Academic Computing Committee (an appointed committee); Illinois Wesleyan has institutional methods of dealing with misconduct for students and faculty; there is a standing Hearing Committee that works with the Personnel Council in cases of faculty misconduct; and the University has a Judicial Review Board for cases involving student misconduct.

Until recently, Illinois Wesleyan University had very little computing on campus. A nearby state university (Illinois State University) serviced the needs of Administrative computing. Faculty computing was not supported. The only academic computer lab contained twenty Tandy, dual floppy computers and three terminal hook-ups to the University of Illinois. There was and is no mainframe on the campus, although the University supports administrative computing via the recent acquisition of an IBM AS/400.

In 1989, the University made a serious commitment to providing computing capabilities to students and faculty. The desktop computing population has grown to about 450 units. Each faculty member has a desktop system. The University renovated a building and created an open-access lab, two computerized classrooms with desktop units available at each student desk, and an interactive learning center to support multimedia courseware development and use. There are also a few special-purpose labs to support specific departmental needs. As noted above, administrative computing now is supported using an AS/400 system. Desktop units are approximately equally divided between Macintosh and PC clone machines. Several classrooms have computerized teacher's stations to support multimedia presentations. The Library has increased its connections with on-line searching facilities and the use of CD-ROM technology. In addition, the University is implementing an E-mail system using the campus digital phone lines and has recently become an Internet node.

The institution has benefitted from its lack of previous computing. There were no old machines to replace, no mainframes in which the University had sunk enormous amounts for support. Other than the connections to the AS/400, the entire campus uses desktop units. In the labs and classrooms, a Local Area Network (LAN) connects the computers. The Academic Computing staff supports all desktop units, manages the labs and classrooms, and performs maintenance and repair on all units.

One of the classrooms is a Writing Workshop. This is a Macintosh-based classroom with 20 student units. All freshmen expository writing students are taught to use these computers as part of their expository writing course. The other classroom is shared by computer science, business, and economics, and sociology. It contains 29 student IBM PC's.

The future of computing at Illinois Wesleyan University is very positive. The University is building a new science building with several computerized labs, several small research computers, and a building network.

Why Was a Policy Necessary?

With this explosion of hardware and software on campus, several new problems arose. When computers were located in one room, it was relatively easy to watch the users and ensure the copyright laws were followed, at least with regard to software. Since no computers were connected to any others, no one could do any damage to all the systems without considerable effort. Of course, it was also possible to monitor use and track problems when they occurred.

The new environment posed two major problems. One was the network integrity in the networked building from both malicious and accidental abuse from users. The other, what was happening across the campus in faculty and staff offices, and software copying. Illinois Wesleyan is not a University with an enormous software budget. Choices had to be made and software purchases were carefully considered. Without infringing on privacy rights and academic freedoms, the institution wanted to discourage its employees from participating in copyright infringement in any form.

For the University, there was also the concern for liability. Some institutions have had to institute policies as a result of criminal prosecutions and lawsuits. While the legal liability of an institution for activities of individual faculty, staff, and students is not completely clear, it is likely that the risk of such liability is reduced by reasonable efforts to control copying.[1]

In addition to all these factors, software companies were becoming more aggressive in their attempts to discourage copyright infringement. It is not the purpose of this article to argue the extent of the copyright law, but it is widely acknowledged that software is protected and cannot be copied freely for classroom use or personal use, much less to spread around the institution.[2]

How the Policy Was Developed

As the need for such a policy became clear, it was the Academic Computing Committee who decided to see the task through to completion. This committee had members drawn from the faculty and administration (including the Manager of Academic Computer Services) and was, therefore, an ideal spot for such discussions to occur. It was decided to appoint a small task force to create the policy which would then be reviewed, edited, and approved by the entire committee. The appointed task force consisted of a Philosophy professor (Dr. Larry Colter). a Computer Science professor (Dr. Lisa Brown), and a member of Academic Computer Services (Marilyn Barnes).

The task force compiled an extensive list of policies implemented at other institutions and used this information as a basis for the IWU policy. The task force determined some underlying principles on which it would base its policy:

1. The policy should be entorceable. Without enforcement, the policy would be useless and ignored. Therefore, the institution had to endorse the policy formally.

2. The policy should respect the ethics of professional colleagues. The policy was intended as a technique for the University to police itself and not as a method for harassing colleagues.

3. The policy had to respect faculty member's, staff's, and student's rights to privacy. So in much the same way as the University has no right to control what one creates with the use of a pen and paper but can protect itself if a faculty member uses that pen and paper to commit sexual harassment or to write threatening letters, it has no right to investigate the works created using the tools provided by the institution (in this case, the hardware and software that comprise the computer system).

4. The policy had to respect the rights of the student users. Forced to use a facility to support classroom assignments, the students would not be coerced to signing an oath.

5. The policy should be legally viable and defend the rights of the institution.

In many ways, this policy was handled in a way similar to the University's sexual harassment policy. Such policies must be implemented by an institution and, while requiring faculty input and participation, are implemented and imposed by the administration for the benefit of the institution. This meant that the task force had to include the comments, where possible, of faculty members and committees, but that the policy itself had to be approved and implemented by the administration and the Board of Trustees.

The task force performed a search for information on such policies in institutions across the country. In looking at policies for approximately forty colleges and Universities, the committee noticed that some policies that sounded good would be unenforceable in a micro-computing environment. Many policies depended on the use of accounts and user identification to establish methods for tracking misuse and for enforcing the consequences mandated by the policy. Many institutions had very rigorous penalties, with dismissal from the institution a very real possibility in policies like that of the University of Michigan. Reading these policies gave the committee the sense that a balance had to be struck between the intimate atmosphere and sense of community encouraged at our campus and the increasingly likely possibility of a case a misuse occurring.

The committee did not confine its research to campuses within the United States or post-secondary institutions. Even public schools were beginning to cope with the problems of software copyrights[3]. Universities in other countries were also exploring the need to improve their policies given the increasing use of software and Internet at their institutions. In all, the committee reviewed well over 50 policies and procedures and participated in some of the Internet discussions concerning such policies.

The committee had one other concern. Not only was it clear that computing was growing on our campus, but because of the lack of a mainframe environment, there were still faculty members (actually increasing numbers of them) who were linking with the University of Illinois Computer Center to perform some of their research computing tasks. It was therefore important for the committee to include some acknowledgement of the University of Illinois Computer Use policy and support-its implementation on our campus.

In drawing up the policy, the Task Force had another choice to make: Should the policy be strictly a legal document, or should it go beyond the strictly legal and vcreate a policy which also emphasizes the moral rights and obligations of staff and students with respect to computer use? Illinois Wesleyan is the sort of institution in which matters of value, of fairness, justice, integrity, etc., lie squarely at the center of its mission. As an institution, we seek to promote and enhance the capacities for and commitment to acting as good citizens of a global community.

The Task Force decided, therefore, that our policy should reflect those institutional commitments, and so the policy that follows immediately below goes beyond the strictly legal issues and focuses on ethical issues as well.

The Policy

Illinois Wesleyan University is committed to the proposition that an academic institution is a community in which the ideal of honesty is to be fostered, encouraged, and achieved. Respect for the University, for one's fellow humans, and for their property - both real and intellectual - are therefore essential ingredients of that ideal, and the University expects of all its members that they exhibit such respect. The ideal of honesty is of course a moral ideal, and so the policy stated below will in some respects go beyond the mere requirements of the law.

Computing technology, because of its extremely volatile[1] nature, presents strong possibilities and hence temptation for misuse. It is doubly important, therefore, for all members of the University community to be aware of that fact and to be doubly committed to use such technology appropriately and to show the respect described above. Accordingly, and for the benefit of all members of the University, the information technology usage policy stated below is intended to make clear just what constitutes that respect, and all members of the University are expected, on pain of penalties described herein, to abide by this policy.

All users of the University computer facilities must agree to use the facilities legally, ethically, and in keeping with their intended use.

1
System Integrity

Actions taken by users which interfere with or alter the integrity of the University's computer system are improper. Such actions include unauthorized use of accounts, impersonation of other individuals in communications, attempts to capture or crack password, attempts to break encryption protocols, compromising privacy, destruction or alteration of data or programs belonging to other users, and attempts to steal or destroy software resident on campus computing facilities. It is improper to create worm or virus programs or conduct experiments to demonstrate computer facility vulnerabilities without prior permission of Academic Computer Services, or to create programs which disrupt or interfere with other users' computing processes. Users are responsible for damage caused by infected software they introduce into the system.

2
Copyright Observance

All users of University-owned computers are expected to abide by copyright laws and licensing agreements. No software should be loaded on any University computer in violation of licenses or laws. No user may copy, or attempt to copy, any proprietary or licensed software provided or installed by IWU.

The University recognizes its role in education for ethical behavior in the computer setting as well as elsewhere. To that end, the Manager of Academic Computer Services will provide, when requested, information about copyright and licensing issued to members of the University community. Said manager will not be liable for copyright or licensing infringements by and student, faculty, or staff member.

The central "fair use" concept of the 1976 copyright law allows borrowing of small amounts of printed, audio, or video materials for such uses as "criticism, comment, news reporting, teaching,... scholarship, or research" [*Copyright Revision Act*, p. 16]. The test of fair use addresses (1) the purpose and character of the abuse; (2) the nature of the work copied; (3) the proportional amount copied; and (4) market effect. Aside from legal issues, users should recognize that the violation of copyright laws with respect to software drives up prices, discourages vendors from offering education pricing, and makes the development of good software a risky investment of the developer's time.

3
Privacy Rights

The University respects every individual's right to privacy in the electronic forum and prohibits users of University computers, including personally owned computers linked via University telecommunications equipment to other systems such as the University of Illinois computer system, from violating such rights. Attempts to read another person's electronic mail, to access another's files, to access electronic records containing information concerning another person, or to use another person's password represent examples of

[1] By "volatile," the University means accessible, replicable (hence stealable), and destroyable.

violation of privacy rights.

4
Courtesy

Anuses of University-owned public access computers may result in the suspension of use privileges. Such abuses include (but are not limited to):

- excessive use of paper,
- making electronic mass mailings,
- using University-owned computers for personal monetary gain (except as such use relates to professional development),
- monopolizing machines,
- and other similar or related abuses.

In addition, University-owned public access computer will not be used for games for other than educational purposes. In general, electronic mail is to be used for academic purposes only. Pornographic, threatening, or nuisance messages are violations of the user's pledge to use computing facilities ethically.

5
Sanctions

The University may take disciplinary and/or legal action against any individual who violates any computing policies, including temporary or permanent suspension of an individual's use privileges to all or part of the college computing facilities, temporary suspension from the University, or permanent separation therefrom. Student violations of academic honesty standards for classwork will be reported to the Office of the Associate Dean in accordance with regulations described in the student handbook

6
Liability

Illinois Wesleyan University hereby expressly and explicitly disclaims any liability and/or responsibility for violations of the policy hereabove stated.

Thorny Issues

There were several topics that created considerable discussion. One of the easiest questions to handle was whether or not to allow the use of games. In the former environment, it was possible to allow controlled game use because the use of the computers could be monitored easily from a single vantage point. In the new facility, it was no longer easy to see what each student was doing. Since the computers were being provided to support academic instruction, the task force felt that students using the computers for that purpose should have priority over students using the computers for recreation. In this particular case, the solution, to not allow games unless used as a simulation or exercise for instructional purposes (such as a foreign language game), was easy to implement as well. The computers in question were all in a single building connected to a single network. No games were provided as part of the network software, so use was effectively prohibited.

There was considerable discussion concerning the use of the computer equipment for monetary gain. While no one felt the University should support someone running a business using the University computers, it was difficult, especially with regard to faculty use, to draw an appropriate line for practice. In this case, the task force used the same standards they might use for pencil and paper supplies provided by the institution. The university continued to support the use of tools provided by the institution in support of faculty research and development that was not funded by another agency. Computing time on other mainframes was also supported within reason. So the task force felt this standard could be used to support the writing of books and papers for publication, etc.

One of the techniques used by software companies to control copying is to provide a limited set of manuals. The task force felt this practice was an excellent way to help enforce the licensing agreements. Most software packages are too complicated to use without some form of manual. Academic Computer Services tracks each piece of software and works to make sure manuals are controlled.

Another area of considerable concern was academic dishonesty cases that occurred in the computer science department. students who would not have considered the possibility of copying someone else's term paper, were not getting the message that a program was also someone's intellectual and creative property. It was considered important to add some statement in support of the computer science department's efforts to correct this misconception and prevent unnecessary occurrences of plagiarism. The original policy had an attachment detailing the events that would be considered as academic dishonesty in the context of software, but this statement has been incorporated in the syllabi of the computer science courses instead.

Implementation

The committee devised, along with the policy, an implementation plan. The first stage of this plan was to obtain the approval of the Board of Trustees. To this end, the task force developed a rationale for the plan - essentially o three page position paper explaining the reasons for such a policy and some of the supporting evidence for the policy. In particular, the task force felt it important to further describe some of the wording of the policy (for example, using University-owned computers for personal monetary gain). This rationale and the policy, accompanied by a member of the Academic Computing Committee, were then sent to each of the major University Councils (Personnel, Curriculum, and CUPP) to request review and comments. The policy and rationale were also sent to the campus attorney, whose comments worked to improve the document and make it more legitimate legally. After the committee included all appropriate comments, the final draft of the policy was presented to the Board of Trustees for approval.

The second stage of the implementation plan was to include the policy in the faculty and student handbooks. The policy was presented to the faculty very successfully thanks to the previous work with each of the Councils and the work of the members of the Academic Computing committee in explaining the plan. It was considered exceptionally important that the Academic Computing Committee was evangelistic in working with the faculty on the plan. This was especially critical because the Academic Computing Committee has as its members faculty from most disciplines and those who are the most current with computing technology in their disciplines. They therefore commanded a certain respect and, if they were willing to live by these rules, it was felt the rest of the faculty would be too.

The third stage of implementation was to begin to make sure that every student was aware of the policy. The committee decided that registration was the best time to hand out the policy. It is at this time virtually every student on campus is seen in one location. Also, it is a place where students are handed a number of such materials. In order to be sure the students could not claim ignorance of the policy, the committee decided each should sign a sheet saying they had red the document and understood its meaning.

The Signature Sheet

Illinois Wesleyan University
Academic Computer Services
Computer Facilities Use Agreement

I, ________________________, am being granted permission to use the academic computing facilities at Illinois Wesleyan University, including, but not limited to, microcomputer facilities in Buck Hall, Sheean Library, and Sherff Hall, telephone and network access, and associated peripherals for academic, non-commercial purposes. permission is also being granted for use, on site, of licensed software.

I have been given, have read, and understand the terms of "Information Technology Usage Policy" which governs the use of such technology at Illinois Wesleyan. As part of that policy, I agree to abide by the licensing agreements between Illinois Wesleyan and the software licensor for software programs, databases, applications, word processing packages, etc. I acknowledge that such software is proprietary, subject to copyright laws, and not available to copy, transfer, or remove from the facilities.

I also agree to abide by the policies of the University of Illinois, or other institutions as applicable, when using facilities controlled by their policies.

I accept full responsibility for enduring that my use of the computing facilities does not interfere with other users or the proper functioning of dais facilities. I acknowledge the right of the Academic Computer Services personnel to inspect and remove, if necessary as a function of responsible system management, any files resident on computer equipment under their supervision.

The Manager of Academic Computer Services may take actions against any violation of this agreement. These actions may include fines for damages, revocation of usage rights at all campus computing facilities, and further disciplinary action as deemed appropriate by the All-University Judiciary Committee, as well as legal action by owners and licensors of proprietary software.

Signed ____ *Date* ____________

It was during this phase of implementation that the committee discovered a small problem in its plans. These sheets were to be returned to the lab desk in the computing lab. However, the campus did not have any way of monitoring the use of the computers to prevent a student from obtaining access without signing the sheet or if they had misused the equipment. The manager of Academic Computer Services has, to this end, worked at securing a magnetic strip reader to read the magnetic strip on the back of the student identification cards. These strips were already used on campus to track students' meal ticket status and other information. To use a computer, a student had to turn in his/her identification card in exchange for a start-up disk. This point of contact was considered the appropriate time to check for the signature and authorization. The purchase of the card reader included the software required to track the student identification numbers.

The Academic Computing staff also installed virus and file protection software where it was most needed. In this case, the Macintosh computers seemed more susceptible to abuse and the Macintosh network less able to prevent such abuse. The PC clone side of the facility was supported using Novell Netware and had more capabilities for protecting files, restricting access, and isolating the user from the system.

In the Office

Academic Computer Services has attempted, where possible, to purchase site licenses of the software most frequently used on campus. Often these licenses are discounted for educational use. Although the University does not mandate a particular desktop platform, personnel are encouraged to use the standard word processing, spread sheet, and database software supported for each platform. In this way, the University reduces the risk of departments purchasing one copy and sharing it among several faculty members. Faculty members have been encouraged to know the policy and contact the Academic Computing Services personnel if they have questions.

Academic Computing also produces a newsletter. This newsletter has been used to inform the faculty and staff of problems and cautions concerning ethical use of computers. The newsletter regularly runs articles defining terms and explaining common misconceptions concerning software. The public relations campaign has been of great service in increasing the support for the Computing Policy among the faculty and staff.

The policy was adopted in April of 1993 by the Board of Trustees of the University. The process of defining a policy was started by the members of the task force in the Fall of 1990. The long time from inception to completion was occasioned by a serious consideration for process. Where possible, the task force strove to include members of the affected communities. This long process has really shaped a new attitude on campus towards software piracy. Although it has really never been too difficult to persuade the user community that serious abuse is improper, there has been a certain Robin Hood attitude towards software piracy and computer hacking. The education of the community in the ramifications of such actions in higher prices, less frequent upgrades, etc. has helped change some of these perceptions.

Another step taken by the committee was to enlist the help of the computer science department in educating the students most likely to violate certain sections of the policy. With repeated support of ethical use of computers in the classroom (as well as modelling this behavior for their students), the computer science department has been effective in stopping some of the abuse before it occurs or causes serious damage. This department works closely with Academic Computer Services and helps identify users who are causing problems.

The Future

Illinois Wesleyan is about to enter a new phase of computing. Plans are under consideration to network portions of the campus. A new science building housing Biology, Chemistry, Computer Science, Math, Psychology, and Physics will be configured as the campus hub. The building itself will have an extensive local area network. The implementation of a network, with its possible connection to administrative computing facilities to help faculty with registration and other administrative tasks, brings with it a new set of potential abuses. It also brings a new set of potential solutions, since version numbers of software can be monitored and updated centrally. The University has planned to work with the software vendors and hardware vendors to ensure the security and confidentiality of the new system.

1.Green, Kenneth C. and Gilbert, Steven W.; "Software Piracy - Its Cost and the Consequences;" CHANGE; Jan/Feb 1987; pp. 47-49

2. Lytle, Susan S. and Hall, Hal W.; "Software, Libraries & the Copyright Law;" Library Journal; July 1985; pp. 33-39

3.Zakariya, Sally Banks; "Play Fair with Publishers, and Put School Software Pirates in the Brig;" The American School Board Journal; March 1985, pp. 38-41