Project Number: MLC-NP00

Case Study in Perception of University Network Use Policy

An Interactive Qualifying Project Report
submitted to the Faculty of
WORCESTER POLYTECHNIC INSTITUTE
in partial fulfillment of the requirements for the
Degree of Bachelor of Science
by

_____

Adam J. Augusta

_____

Michael A. Narris

Date: November 12, 2001

Approved:

_____

Professor Mark Claypool, Major Advisor

_____

Professor Robert Kinicki, Co-Advisor

Abstract

Non-academic use of high-speed academic networks has altered formal network use policies and the methods of enforcement on networks in the academic community. This project surveys students at selected competitive colleges on their network use and their perceptions and opinions regarding their college's network use policy and it's enforcement. The survey responses demonstrated that the attitude and behavior of students are affected by their college's network use policy.

Table of Contents:

I. Introduction……1

II. Background……3

III. Methodology……..12

IV. The Survey……16

V. Requesting Permission to Survey Students……... 24

VI. Data Analysis Methodology…….. 31

VII. Survey Results and Data Analysis …… 32

VIII. Conclusions……61

IX. Future Work……...65

Appendix

A. Interview questions……...67

B. Sample survey……...68

C. Form letters……... 73

D. College web page URLs and addresses…… 79

E. Acceptable network use policies……...80

E.1 Worcester Polytechnic Institute Network Use Policy…..……...80

E.2 Clark University Network Use Policy …...……... 89

E.3 Illinois Institute of Technology Network Use Policy…… 92

E.4 University of Chicago Network Use Policy……... 96

E.5 Georgia Institute of Technology Network Use Policy…….. 104

E.6 Emory University Network Use Policy……. 116

E.7 Harvey Mudd College Network Use Policy…….. 118

E.8 Pitzer College Network Use Policy……... 122

Bibliography……... 125

I. Introduction

The introduction of high-speed information transfer has left a wide variety of legal and social implications in its wake. File sharing services such as Napster[1] were the focus of lawsuits by copyright enforcers. Before this transformation, the system administrator needed only to concern himself with the continuing operation of his network. In light of recent developments, an administrator is now forced to determine what kinds of content can be transferred to whom and is making decisions that alter the scope of modern use.

Many college communities have campus networks, which, while traditionally used for academic purposes, have more recently fostered a wide array of uses, from online communication to extensive file sharing on an unprecedented scale. As the college community makes greater use of campus networks, administrative decisions that affect the scope and environment of that use have increasing potential to modify the types of communities that form on campus.

The need for socially oriented network use policies, as opposed to policies that set technical guidelines for equitable use, is a relatively new one, and the resulting impact may neither be obvious nor easy to determine. Lacking precedent in dealing with the implications of socially oriented policy, administrators have little basis upon which to structure their policy decisions, and are often forced to rely on more mundane measures such as bandwidth limitation and pressure from higher administration. A more deliberate approach to determining the effects that policy has on the diverse and manifold use of interactive networking may help in making these decisions. Such a study would help determine the impact that computer networking actually has in a student's life, and hence determine what policies could affect the things that have become important to a student.

The purpose of this project was to determine any effects that recent changes in policy have brought upon the academic community and its students as a whole. The project also examined the differences among colleges in various regions of the country, as well as differences within the individual colleges such as those found among classes and between genders. To establish these differences, eight colleges within the United

States were selected and contacted for the purpose of distributing detailed surveys to their students.

In colleges across the country, a wide variety of network use policies are in effect. An examination of network use and opinions of students at these colleges may allow examination of the impact of these policies on student use. Student opinions as well as an examination of their behavior are important indicators of policy impact. Students' familiarity with the policy and its availability indicate how effective the college administration is in educating their student body about its network use policy.

One would expect different colleges with different socio-political backgrounds to handle modern issues of network use differently. For example, the policies of colleges in different regions may vary with respect to the socio-political climate surrounding each college. Students themselves may also have different motivations and hence make different use of the network based on the local culture. There may also be a difference in the patterns of use among various classes due to differences in network experience and also between genders due to varying interests. Other issues may impact the students and network policy makers, such as the type of college, be it liberal arts or technical. Differences may be found among the various academic classes, student gender, and even student computer experience.

This paper details various related projects in the past, the methodology of all stages necessary to get a detailed survey into the hands of students, and the analysis of the data gathered and resulting conclusions. Section II, Background, discusses previous related projects and their impact on the decisions made with respect to the methods and procedures of this project. Section III, Methodology, discusses the choices and steps involved in developing and deploying the project survey. Section IV, The Survey, details the reasoning and subsequent development of the final survey, and what was expected of each question. Section V, Requesting Permission to Survey Students, deals with obtaining permission to distribute the survey to students at various colleges. Section VI, Data Gathering Methodology, explains the process used to compile the data in a useful format for analysis. Section VII, Survey Results and Data Analysis, overviews the set of results and discusses the significance of the responses to each question within the survey.

Section VIII, Conclusions, details the conclusions drawn from the results of the analysis. Section IX, Future Work, discusses how the results and insight gained in this project can be used to further achieve the overall goals of this project.

II. Background

This section discusses several topics pertinent to our approach in discovering the impact of network use policies and enforcement on student opinion and behavior. Establishing the original intent of campus networks provides insight with respect to the foundational motivations of maintaining such networks. Previous academic research helps show how campus network use evolved concurrently with the campus networking technology. Previous studies also provide insightful commentary on how best to approach academic research in this project. Legal issues both recent and traditional have an impact on student behavior and network use policy. The importance of academic communities in industry, research, and politics makes it quite clear that any impact of policy on student use could, in turn, impact society as a whole. The section goes on to detail the network use policies of colleges examined in this project in order to provide a general sense of what these policies entail, as well as provide background for any differences discovered between the colleges.

Academic computer networks have been a pertinent issue since the mid-seventies. At that time, distributed systems were being formulated and created as an economical necessity in order to balance the cost of computing power against the number of people using the resources[2]. In fact, prior to the introduction of the ARPANET, many colleges almost exclusively provided these resources with minimal federal grant support. With the increasing applications of computers in the eighties, computing was a necessary expense, and with the advent of popular networking technologies like TCP/IP, the use of computers has increased and developed into the extensive network structure we see today in colleges across America.

In the early eighties, there was a wide proliferation of personal computers. The original goal of networking was the economical distribution of processing power. Paradoxically, the increased processing power provided to individual students through personal computing did not decrease but rather increased the level of networking on campuses. By 1982, students on approximately 400 autonomous networks were busy publishing notes and articles on a series of forums collectively known as Usenet[3]. It became quite clear that academic networks had evolved into a social medium as well as

an academic one. A study done by Linnda R. Caporael indicated that computers did not necessarily make students better at their tasks, as grades could not be correlated with computer use[4]. On the other hand, the high-powered personal computer was still used as an interface to communicate and perform work on the mainframe while its local resources were largely predisposed to individual uses such as video games, word processing, and personal computer-related projects.

Modern computing takes on a variety of forms on college campuses. Network connections are increasingly found in many aspects of student life from dorm rooms to classrooms and school labs to student recreational facilities. Even among smaller, local community-oriented colleges, professional high-speed connections are found, and over 180 universities are working in partnership with industry and government to develop and deploy Internet2[5], an advanced suite of network applications and technologies, to ensure the rapid transfer of new network services and applications to the broader Internet community.

These levels of connectivity give students access to unprecedented information, multimedia content and communication. Students have access to information from how the Earth formed to how to perform almost any task. The World Wide Web and suites of readily available Internet applications provide students easily access music, e-books, and even movies. Students can communicate with friends and family at little or no cost and can readily access information for academic research.

The versatile use of campus computer networks can be impacted by network use policies. In order to assess that impact, it is necessary to examine the activities of students on these high-speed networks as well as the students' opinions. Students of all ages have been a prime demographic in many sociological and marketing studies. This project employs the lessons learned in these studies in an attempt to achieve effective and pertinent student research.

A major aspect of student studies is determining how best to collect data. A study done by Gregory Jackson points out that there are several means of evaluating learning technology, which include surveys, interviews, observation, and activity measures[6]. Surveys are designed to document activity, but only indirectly. Students can be asked to list computer activities, but students tend to forget some activities or leave out

recreational or illegitimate uses. Students may also be poor at estimating the time spent on their practices in retrospect. Interviews, while more flexible, tend to be less consistent in determining trends, but can be more insightful by allowing follow-up questions on points of interest. Jackson indicates that for determining social effects and attitudes, surveys and interviews prove the most effective means of data collection. For actual determinations of use and consequences, observation works well in coordination with those methods, however it is more difficult to achieve.

A study by John Walsh indicated that surveys distributed remotely by computer are more effective in ascertaining student opinion and network use than surveys given through other forms of distribution[7]. Because computer surveys convey little social information, respondents experience less evaluation anxiety than when they respond in other forms of survey administration[8]. This, combined with the fact that completing electronic surveys is as easy as responding to e-mail, can improve response rates and increase self-disclosure. Participants are more likely to respond to e-mail surveys because the survey is on-line, easy to access, and easy to answer. Surveys that are relevant to the community in which they are involved and to topics about which prospective respondents have knowledge and opinions are also more likely to garner responses.

With the fast and rapidly increasing levels of information exchange over campus networks and the Internet as a whole has come many social implications that have threatened to change the paradigm of copyright law. Free access to copyrighted material, such as music, e-books, and even movies has become readily available to anyone with high-speed network access. In response to these modern changes, new laws have been put into effect to hamper widespread piracy. The widest reaching among these is the Digital Millennium Copyright Act of 1998 (DMCA)[9], which prohibits circumventing technological protections put in place on copyrighted material. Massachusetts Computer Crime Law[10] and conventions in other states hold that data legally constitutes property.

In response to these laws, some colleges have made major changes to policy, limiting the use of file sharing services, such as Napster and Gnutella[11]. Other universities have come out adamantly in support of these file-sharing services, citing concerns over censorship and academic freedom. In a written statement, Duke University

said it was "committed to fundamental principles of academic freedom and the uncensored dissemination of knowledge and information… there are legitimate educational and other non-infringing uses of Napster."[12] With time and the advent of increased litigation, these file-sharing services have grown more widespread and fragmented, and the academic community maintains no definite position on the issue. This may change with future precedent in court cases, as it is still unclear what legal responsibility the college, as an Internet service provider, has in regulating student activity[13].

Campus networks have been the basis for pervasive academic communities. Academic clubs coordinate plans and increase community participation through extensive use of electronic correspondence. Many student organizations actively and independently publish various content from computer science journals to college newspapers electronically. One such example of an independent publication is The Harvard Crimson Online Edition[14], a reputable source of news, opinion pieces, and other media. Major organizations such as the ACM maintain independent chapters throughout colleges in related fields of study, which largely maintain their infrastructure through electronic correspondence. Virtual academic communities of people such as the ACM and its satellite chapters have grown in recent years, and have become more involved in industry, academic research, and politics. As they become more pervasive, these communities can be expected to have a larger impact on society.

Restrictions on how students interact can have a profound impact on the type of communities that are created. Restriction can take on a variety of forms including written guidelines, selective enforcement both preventative and penal, and vocal discouragement, each with varying effects and levels of effectiveness. The only one of these restrictions that can be explored without gathering new data is that of the written network use policy. Below is a summary of the written policies from each college used in this study, as selected and identified in Section III, Methodology. The policies in their entirety are included in Appendix E.

In this project a standard network use policy is a written statement that prohibits non-academic behavior that may impede teaching and research, activity prohibited by law, and abuse of the system and its users. Many colleges list examples of possible

violations but in general, what constitutes a violation is left to the discretion of the administrators, in order to cover all possibilities.

Worcester Polytechnic Institute Acceptable Network Use Policy[15] Overview:

Worcester Polytechnic Institute (WPI) uses a standard policy, which is updated regularly, that outlines in detail what is absolutely not allowed. The computing resources are in place for academic uses and any disruption of these uses is a violation. Commercial activities, misuse of copyrighted material, abuse of email systems, violating other users' privacy, and violations of the Massachusetts Computer Crime Law all may result in loss of privileges or possibly even civil or criminal prosecution.

Clark University Acceptable Network Use Policy[16] Overview:

Clark University's policy is a standard policy addressing what is not acceptable on their network. Users must abide by all laws including copyright laws, as well as rules instated by administrators. The policy clearly states that it is made available to every student, handed to every new user, and posted in all the labs. Policy offenders are emailed about violations and asked to cease the illegal activity. In the event of a more serious violation or repeated violations, cases will be referred to regular disciplinary channels along with relevant information and evidence.

Illinois Institute of Technology Acceptable Network Use Policy[17] Overview:

Illinois Institute of Technology's acceptable use policy is a standard policy that lists examples of improper conduct. Users are allowed to have opinions but are not allowed to harass or discriminate other users. They are not allowed to attempt to monitor or break into other computers, pass on harmful applications such as viruses, circumvent security, or perform acts that would waste computing resources such as sending mass mailings or chain letters, creating unnecessary multiple jobs or processes, obtaining unnecessary

output, or printing or creating unnecessary network traffic. Violators are subject to network suspension, and the matter may be referred to the campus judicial board.

University of Chicago Acceptable Network Use Policy[18] Overview:

University of Chicago uses a standard network use policy that details how the college's resources are to be used. "Restricted applications of University information technology primarily include those that threaten the University's tax-exempt status, such as certain kinds of political activity and most commercial activity, those that are illegal, such as fraud, harassment, copyright violation, and child pornography, those that deprive other users of their fair share of University information technology or interfere with the functioning of central networks and systems, such as mass mailings, chain letters, unauthorized high-bandwidth applications, or denial-of-service attacks, and those that violate more general University Statutes, Bylaws, and policies." A memo was also released stating that digital music sharing programs such as Napster were violations of the policy and of the Digital Millennium Copyright Act, 105 PL 304. Violators are subject to disconnection from the network, police intervention, or legal action.

Georgia Institute of Technology Acceptable Network Use Policy[19] Overview:

Georgia Tech has a fairly strict general policy. Prohibited activities include harassment of other users, harmful activities, unauthorized access, unauthorized monitoring, academic dishonesty, use and distribution of copyrighted information and materials, political campaigning, commercial activity, personal business, attempts to circumvent security, or decoding access control information. The policy also states that the network is not completely private, and that monitoring and logging of network activity occurs by the administration. First time and minor violators of the policy will be given a copy of the policy to read and sign. Subsequent violations or major violations will result in the violator being subject to "sanctions including the loss of computer or network access privileges, disciplinary action, dismissal from the Institute, and legal action. Some

violations may constitute criminal offenses, as outlined in the Georgia Computer Systems Protection Act and other local, state, and federal laws."

Emory University Acceptable Network Use Policy[20] Overview:

Emory University's policy states that any activity that impedes teaching and research, hinders the functioning of the university, violates an applicable license or contract, or damages community relations or relations with institutions with whom we share responsibility, is a violation. Violators may be subject to suspension of network privileges, university disciplinary procedures, or in extreme cases, criminal prosecution.

Harvey Mudd College Acceptable Network Use Policy[21] Overview:

Harvey Mudd College (HMC) uses a standard acceptable use policy listing many examples of possible violations including wasting computing resources intended for academic purposes. It is stated that users must avoid wasting these resources by excessive game playing or other trivial applications; by sending chain letters or other frivolous or excessive messages locally or over an attached network; and by printing excessive copies of documents, files, images, or data. Users are also prohibited from disrupting others work or abusing other users. Violations of appropriate use may result in one or more of the following actions:
"A written warning to the offender, a restriction of system access for a specified term, a revocation of all system privileges for a specified term, or a statement of charges to the appropriate disciplinary body at the student's home college, which could lead to other penalties up to and including probation or suspension."

Pitzer College Acceptable Network Use Policy[22] Overview:

Pitzer College uses a standard policy prohibiting questionable non-academic activities. Users may not violate copyright laws, use the resources for commercial use, or engage in

abuse of other users. Violators are subject to loss of computing privileges, deactivation of accounts, and removal of network connection.

III. Methodology

Approach

This section discusses the choices and steps involved in developing and deploying the project survey. The approach of this project involved four aspects. The first was to interview local WPI administrators to get a sense for the current network issues and the measures necessary to regulate and monitor network activity. A second aspect involved determining how to choose colleges around the nation in order to achieve the most diverse representation of comparable data. Once the test cases were chosen, professional administrative contacts needed to be established in order to obtain permission and a method to distribute the project survey to each college. The fourth aspect involved developing the survey itself.

Interviewing local academic administrators:

Two local WPI network administrators were anonymously interviewed. Please note that all contacts have been kept anonymous to help alleviate any concerns of administrative accountability, as well as to further demonstrate to potential contacts that this survey was not intended to provide a critical review of the college itself, but rather to discern the differences between different types of colleges, policies, and methods of enforcement. A series of open-ended questions were composed regarding the college's network policy, any monitoring systems that were in place, and the respective administrator's opinion of several contemporary issues. See Appendix A for the list of interview questions. These questions served as a base for other questions that developed as the discussion proceeded. The results of these interviews provided useful insight in formulating the questions and expectations of the survey.

In practice, the interviews tended to proceed as follows. First, the administrators would be asked what they felt were the major responsibilities in monitoring traffic. Following that, they were asked to go into detail regarding what technical implementations were in place to help them perform their tasks. Those questions would then be followed up by asking about the penalties in place for violations, as well as an attempt to find out what kind of reactions students have to these policies. The administrators were then asked to share how their policies compared to other colleges'

policies in terms of strictness and general philosophy. The discussion then turned to the use of the network, regarding general use as well as the level of use by the academic community as a whole. The last step of the interview was to determine what the major motives are behind the enforcement of policy, whether it be to limit bandwidth or to keep the focus on academic use.

Selecting Colleges to Survey:

In an attempt to limit the number of differences between the colleges, pairs of technical and liberal arts colleges were chosen in the same city, each of which was a private college with no religious affiliation, all with U.S. News overall rankings[23] centering around second tier colleges. The implication of this grouping was that the colleges were all in the same academic league and would attract students of similar academic backgrounds. Other variables preserved across the set of colleges include student body size, a similar tuition rate, and urban setting. All colleges had the financial resources necessary to create a well-designed technical infrastructure.

These pairs of colleges were chosen to split the country into the following four geographical regions. These four geographical regions capture major socio-political differences within the United States without exceeding the scope of the project by ascertaining more minor differences between, for example, adjacent states.

	City	Technical College	Liberal Arts College
East	Worcester, MA	Worcester Polytechnic Institute	Clark University
Central	Chicago, IL	Illinois Institute of Technology	University of Chicago
West	Claremont, CA	Harvey Mudd College	Pitzer College
South	Atlanta, GA	Georgia Institute of Technology	Emory University

Figure 3-1
Pairs of colleges by geographical region

Generating administrative contacts:

Administrator permission was necessary in order to distribute e-mail surveys [see Section IV, The Survey, for distribution details] to large numbers of students at each college. Administrator assistance was likewise necessary in obtaining the requisite list of e-mail addresses. The administrative contacts were found by searching each college's

online staff directory. As a means of immediate communication, e-mails were sent in order to establish first contact to people believed to be in a position to authorize the distribution. If an administrative contact could not be established though subsequent emails or by changing the potential contact, the next course of action was to make phone calls to ask for permission.

Developing the survey:

To create a survey, several items needed to be taken into account. The first of these was the formatting of the survey. Compatibility between e-mail clients was necessary, for recipients use a wide variety of mail clients. Also, a consistent layout of questions and entry boxes was necessary in order to increase the ease of completing the survey, as well as allowing for easier extraction of the data.

The second major issue to consider in the general layout of the survey was survey length. The survey needed to be short enough to be completed within ten minutes, while still effectively encompassing the scope of the project. After careful consideration, the team decided on 10 form questions in addition to one open-ended question to keep the time required to complete the survey at about 5-10 minutes. The survey underwent 12 iterations of changes to content, wording, and layout before the team decided the survey met these goals.

Deployment

The next stage of the process involved the deployment of the survey. This included the deployment of a pilot study, which was used to determine any shortcomings in response or question quality. The second stage of the process involved guaranteeing an appropriate level of response in the final surveying. The timing and framework of the survey's distribution is discussed in Section V, Requesting Permission to Survey Students.

Pilot Study:

A pilot study was conducted for the following purposes. The first was to ensure that the survey would provide meaningful data. The time required to complete the survey

was recorded to ensure that completing the survey did not require too much time. In order to determine if the survey took too long to complete, 10 participants casually selected from both WPI and Clark University were asked to record the time they spent filling it out. The participants were also asked to share their insight on the wording of each question, as well as the clarity of each question's meaning. The variation in the answers could then also be examined to determine whether each question's meaning was being interpreted properly. Lastly, the study was used to get some sense of the expected response rate. Completion times fell within the target range of 5-10 minutes. In order to clarify the meaning and intent of some questions, minor alterations were made to the wording of the survey as a result of this pilot study.

Response Rate:

The response rate for this type of survey ranges between 10-30%[24]. The goal of this survey was to acquire enough student results to appropriately represent the study body. The figure selected for the number of recipients was originally 100 students per college. For reasons explained in Section V, Requesting Permission to Survey Students, this number was later increased to 500. To increase the response rate, the survey was redistributed to non-responding students 72 hours after initial deployment. The design of the survey itself was also intended to increase the response rate by allowing students to quickly and easily fill out the provided survey as explained in the next chapter.

IV. The Survey

This chapter deals with the creation of the survey, the design decisions behind it, and a question-by-question overview. Besides the instrumental goals of determining what types of questions need to be asked, there are many secondary goals that are necessary to increase response rate, reduce response time, and make for easy extraction of survey results.

The first of these goals was determining the type of distribution. There are several methods of distribution, including mail, personal distribution of paper copies, web-based distribution, and e-mail distribution. The cost and time required for widespread mail distribution to colleges countrywide, as well the administrative hassles of getting paper copies of the survey distributed to all students within each college proved prohibitive. The problem with web-based distribution was that it presents a second step to the user, requiring them to enter a link into their web browser to begin their survey. Due to the extra steps involved, students would be less likely to engage in the survey immediately, negatively affecting the return. E-mail distribution is fast, discloses little personal or social information about the participant beyond the questions asked, and is as easy as replying to regular e-mail, hence e-mail was chosen as the method of distribution for the survey.

The survey needed to be designed to be compatible with most e-mail clients. Some e-mail readers such as Microsoft Outlook and Eudora for Windows based machines automatically format text for readability. Other readers such as Pine and Elm for the Unix systems have a set character limit and mail can become difficult to read if the lines are not kept within those boundaries. In order to maintain compatibility across the widest range of platforms, the width of the survey was limited to 75 characters.

Also important was the goal of making the survey easy to answer. Each answer was placed between a set of brackets that preceded each question, allowing the students to enter their answers without excessive side scrolling while providing a consistent format for entry. This made it easier for students to fill the survey out, while the brackets allowed for easier extraction of data. The only exceptions to this were the open-ended questions for which a series of lines were provided immediately after each.

While it was important to cover all the project goals detailed in chapter I. Introduction, it was also necessary to ensure that the survey was short. A long survey can have a large negative impact on the response rate. With this in mind, the survey length was set at ten questions, plus one open-ended question and space for any additional comments the respondent may wish to share on the topic. A pilot study of ten WPI students determined that the survey would take the respondents between five and seven minutes to complete.

One of the dangers of creating questions is having an inherently likely answer, such as middle-of-the-road or thoughtless answers. To avoid this, typically even numbered sets of answers without a 'neutral' answer (e.g. Fair, Acceptable, Unfair) were used, forcing respondents to make the best approximation of their own viewpoint.

In distributing the survey, students may be inclined to procrastinate which can lead to often-indefinite delays. To counter this and increase the number of returns, a timeframe of 72 hours was specified on the survey. After the 72-hour period, the survey was redistributed to the students who had not responded to the first distribution set. Maintaining a strict timeframe of 72 hours between the first distribution and the redistribution to recipients who failed to respond to the first distribution was also necessary to avoid skewing of the data by changes in current events. A complete copy of the project survey is included in Appendix B.

The following section is a detailed explanation and rational of each question in the survey.

Survey Demographics:

```
Demographic Information

School:

[ ] Harvey Mudd College              (Claremont, CA)
[ ] Pitzer College                   (Claremont, CA)
[ ] Emory University                 (Atlanta, GA)
[ ] Georgia Institute of Technology  (Atlanta, GA)
[ ] Illinois Institute of Technology (Chicago, IL)
[ ] University of Chicago            (Chicago, IL)
[ ] Clark University                 (Worcester, MA)
[ ] Worcester Polytechnic Institute  (Worcester, MA)
[ ] Other, please specify:


Gender:

[ ] Male
[ ] Female


Class:

[ ] 1st year student
[ ] 2nd year student
[ ] 3rd year student
[ ] 4th year student
[ ] Other
```

The survey consisted of a brief demographics section, which asks the student which college they attend, their gender and their college year in order to gather some basic information about who was completing the survey. The respondents were asked to indicate which college they were attending, despite the fact that each survey was customized to the college it was sent to. It was determined that a list of all the selected colleges being present would convey a sense of importance and truthfulness to the respondents and positively affect the number of returns. In the event that a student transferred to a different college, they could specify that in the "Other" field and the questions would still pertain to the college intended in the survey.

Providing a detailed list of demographics provides students with a sense that they as an individual will be well represented within the survey, which should positively affected the number of returns. Information provided by gender and class can be used when correlating data to determine differences between the genders and between classes within and across each college.

Survey Questions:

In the instrumentation of the survey, the project needed to cover several key facets. The first was to gauge the student's actual use and behavior. The second involved determining how comfortable the user was with using the college's network for different activities. The third was to gauge their sense of restriction on their use. Lastly, the student was asked to share their opinions on the actual restrictions and enforcement of their college's policy, along with any other perceptions they might think noteworthy.

```
1. In the brackets below, enter the average number of hours per day you
   spend accessing the Internet through:

[  ] Worcester Polytechnic Institute's Network
[  ] Home Connection
[  ] Workplace Facilities
[  ] Other


2. In the brackets below, enter the average number of hours per day you
   spend on each of the following activities:

[  ] Email
[  ] Other Internet Communication (e.g. Instant Messenging, Chat)
[  ] Academic Web Browsing
[  ] Shopping Online
[  ] Other Non-Academic Web Browsing
[  ] Downloading Music
[  ] Downloading Software
[  ] Downloading Other Media
[  ] Playing Network Games
[  ] Sharing Music
[  ] Sharing Software
[  ] Sharing Other Media
[  ] Hosting Network Games
[  ] Hosting Commercial Websites
[  ] Hosting Non-Commercial Websites
```

Question #1 was designed to find out how many hours per day a respondent uses the Internet and from where they access the Internet. Question #2 determines which activities the respondent engages in while accessing the Internet and the number of hours per day they spend on each.

The answers to question #2 were grouped into two major categories: active use and inactive use. Active use consists of communication, browsing, and downloading, while inactive use consists of activities that require no user participation such as sharing and hosting. Sharing is a common term for the inactive distribution of media over a

network where any number of other users on the network can access the shared material. The term "Other Media" is intended to include all other media such as e-books, movies, and images.

```
3. Do you feel in any way limited in your self-expression or expression of
   opinion online (e.g. e-mail, web pages, online communication)?

[ ] Not Limited
[ ] Somewhat Limited
[ ] Limited
[ ] Severely Limited


4a. Are you comfortable with giving out private information over Worcester
    Polytechnic Institute's network (e.g. address, credit card numbers,
    social security numbers)?

[ ] Yes
[ ] No

4b. Are you comfortable with giving out personal information over Worcester
    Polytechnic Institute's network (e.g. medical history, legal records)?

[ ] Yes
[ ] No
```

Questions #3 and #4 are designed to capture whether the respondent feels their activity on the college's network is being monitored or watched either by authorized administrators or hackers. It can be expected that there may be more concern for this at the technical colleges than at liberal arts colleges. Students may feel limited in their self-expression in email and online communication if there are stated limitations or if they feel that someone other than just the intended recipient will read what they are sending. There may be limitations in place on the voicing of certain opinions or other forms of expression on student web pages as well.

The feeling of network insecurity could result in students not being willing to send private information over the network such as their address, credit card number, or social security number. However, some students may be willing to send private information assuming that whoever may be watching is trustworthy and would not misuse the information. These students may still feel they are being watched and might not want to send personal information out over the network such as medical history or legal records for fear of character defamation or other personal repercussions. Even if the use policy says nothing about network use monitoring, a student may have strong impressions that such activity occurs on his or her college's network.

```
5. In what ways are you aware that Worcester Polytechnic Institute's
   Network Use Policy has been made available?  'X' all that apply.

[ ] Available paper copy (e.g. library)
[ ] Distributed paper copy (e.g. orientation)
[ ] Published on-line
[ ] Word of mouth
[ ] Not published
[ ] Other
    Please specify
    >


6. Indicate your familiarity with Worcester Polytechnic Institute's
   published Network Use Policy?

[ ] Completely unfamiliar
[ ] Somewhat unfamiliar
[ ] Somewhat familiar
[ ] Very familiar
```

It is presumed that, published or unpublished, all networked colleges have some sort of acceptable use policy, which specifies what is acceptable and what is prohibited on the campus network. Question #5 asks in which ways respondents are aware that their college publishes its acceptable use policy, if at all. Question #6 determines if respondents have any knowledge of their college's acceptable use policy. If they have any knowledge of the policy then they continue on and answer questions #7-9. Otherwise their answers to questions #7-9 would not be relevant, as they require knowledge of the policy restrictions, and the respondent is instructed to proceed to question #10.

```
7. For each of the following, type an 'X' in the box that indicates whether
   there are actively enforced restrictions placed on each activity on
   Worcester Polytechnic Institute's network.


Yes No  Unknown

[ ] [ ] [ ]    Email
[ ] [ ] [ ]    Other Internet Communication (e.g. Instant Messenging, Chat)
[ ] [ ] [ ]    Academic Web Browsing
[ ] [ ] [ ]    Shopping Online
[ ] [ ] [ ]    Other Non-Academic Web Browsing
[ ] [ ] [ ]    Downloading Music
[ ] [ ] [ ]    Downloading Software
[ ] [ ] [ ]    Downloading Other Media
[ ] [ ] [ ]    Playing Network Games
[ ] [ ] [ ]    Sharing Music
[ ] [ ] [ ]    Sharing Software
[ ] [ ] [ ]    Sharing Other Media
[ ] [ ] [ ]    Hosting Network Games
[ ] [ ] [ ]    Hosting Commercial Websites
[ ] [ ] [ ]    Hosting Non-Commercial Websites
```

Question #7 is designed to determine if there is any known enforced restrictions or perceived restrictions on various specific types of network usage. The respondents should have a relative idea about any restrictions on these activities if they answered that they were familiar with the acceptable use policy in question #6. Any perceived restriction, whether or not it is written or enforced, can have an impact on student behavior.

```
8. How would you rate Worcester Polytechnic Institute's Network Use Policy?

[ ] Lenient
[ ] Somewhat lenient
[ ] Neutral
[ ] Somewhat strict
[ ] Strict

9a. I feel Worcester Polytechnic Institute's Network Use Policy is:

[ ] Unfair
[ ] Somewhat unfair
[ ] Neutral
[ ] Somewhat fair
[ ] Very fair

9b. Briefly express the reasons for your choice in 9a.
>
>
```

Question #8 asks the respondent to rate their college's network use policy in terms of its respective leniency or strictness. This is done to determine how the respondent feels their college's published policy restrictions compare to other colleges' policy restrictions. The respondent might feel that the policy prohibits or allows more activities than other colleges. Question #9 asks if a respondent feels that the policy is fair. Some students may understand why things are the way they are and feel that it is a strict policy but perceive the policy as fair. Others may think that that they are being restricted in activities they feel should be allowed more freedom. Question #9b is the first open-ended question for respondents to express why they feel the policy might be fair or unfair.

```
10. How would you rate Worcester Polytechnic Institute's overall
    enforcement of the Network Use Policy?

[ ] Not enforced
[ ] Lightly enforced
[ ] Neutrally enforced
[ ] Heavily enforced
[ ] I do not know
```

Question #10, which was answered by all respondents, determines what the respondent knows or personally senses about the enforcement of the colleges network use policy. Even if the respondent knows nothing about their college's acceptable use policy, he or she may still know about the enforcement by word of mouth or by knowing an offender.

```
11. Briefly express the most obvious way the Network Use Policy has
    affected your use of the network, if at all.
>
>

Any other comments you wish to make about Worcester Polytechnic Institute's
Network Use Policy:
>
>
```

Question #11 is an open-ended question that asks the respondent to indicate how their college's acceptable network use policy has affected their behavior on the network or any other way it has affected them. The survey then concludes with a general open-ended question for any additional comments respondents might have about the survey or the project in general, to account for any pertinent information that may not have been covered specifically in the questions of this survey.

V. Requesting Permission to Survey Students

This section details the approach and obstacles encountered in obtaining permission of the network administrators at each college along with a case review of all correspondence. During the creation of the survey, permission to distribute the email survey to students needed to be established to prevent possible policy infringement and other violations. The network administrators also needed to provide lists of email addresses, mailing aliases, or another channel of distribution.

An appropriate administrative contact was considered to be an employee in the Information Technology department or the computer systems department with an administrative title. Browsing the computer department's respective web pages for employee information and searching the college's staff directories for contact information resulted in the initial administrative contacts. Once an administrator was chosen and their contact information such as name, email address, and phone number were in hand, the initial request letter was sent to initiate correspondence.

The request letters that were sent to the administrators needed to explain the nature of the project and what was being requested, while providing a list of options in fulfilling the request. A copy of the survey, customized for each college, was included with the request letter for the administrator to review. A URL was also included which linked to the project website which included a copy of the original proposal, a copy of the survey, and links to advisors' web pages. A copy of the initial request letter is included in Appendix C.

In order to achieve an equitable spread of respondents, the 100 requested email addresses needed to be completely random to prevent skewed data such as only one class responding. It was left up to the discretion of the administrator to which method they chose to make the email addresses available. An administrator could opt to send a list of specific email addresses, an email alias such as 'surveyrecipients@college.edu' where the administrator populates the alias without disclosing specific email addresses or they may opt to distribute the survey to the students themselves without disclosing any addresses.

Upon completion of the final draft of the survey, the request letters were sent to the initial administrative contacts at the eight colleges. After answering any concerns

raised and further attempts to establish an appropriate administrative contact at each college, permission was eithergranted or denied by each administrator contacted.

In some cases the person first thought to be an appropriate contact turned out to not be or felt they were not in the position to authorize the distribution of the survey. Through the help of the first administrative contact or through further searching on the college's web site, additional administrative contacts were chosen until the appropriate person was found. In other cases, no response was received for an administrative contact and the request letter was sent to additional staff members until a response was received regarding permission or the name of the appropriate administrator.

Additionally, some colleges may have a policy against handing out student email addresses. This was among the reasons for allowing administrators to choose their method of distribution. However, policy may still restrict or otherwise prevent the distribution of mass emails to students.

The following is a case review of the correspondence with each of the eight colleges included in this study. Included in this review is a table of responses for each college.

On April 14th, 2001, an initial survey request was sent off to each of the eight colleges in hopes of acquiring permission to distribute the survey before the end of the academic school year. On April 19th, a follow-up letter was sent to those who did not respond to the first request letter. Initially only two colleges, WPI and Emory University accepted the request to survey students. 27 WPI students completed the survey, however only 5 Emory University students competed the survey, which proportionally was not adequate for a valid study. The fall semester was the next available academic semester to survey students. As a result, administrators could be established over the summer, providing more opportunity to correspond with the individual colleges.

Attempts to acquire permission for distribution in the fall semester began on July 26th, 2001 when the request was again sent to the eight colleges. This letter was resent on August 11th, 2001 to those administrators who had failed to respond. A phone call was made to each administrative contact that had failed to respond following the second survey request on the week of August 27th. Further attempts to contact the administrators were made to those who continued to fail to respond. Different administrative contacts

were chosen within each college as necessary. See Figure 5-1 for accepting colleges and the following case review by college of the correspondence with administrative contacts.

On September 6th, a deadline of September 10th was sent to the administrative contacts, after which the college would be considered as having declined. In a final effort to acquire permission from undecided administrative contacts, an offer was made on September 13th to generate the e-mail addresses independently of the administrators through their college's public online e-mail list services. The motive behind this initiative was to acquire a definitive yes or no answer by reducing the effort required by the administrator in approving the survey request. See Appendix C for copies of an example of each letter sent.

	Accepted
Worcester Polytechnic Institute	Yes
Clark University	Yes
Illinois Institute of Technology	No
University of Chicago	No
Georgia Technical Institute	No
Emory University	No
Harvey Mudd College	Yes
Pitzer College	No

Figure 5-1: Colleges accepting the fall survey request

The following is a case review by college of the correspondence with administrative contacts regarding permission to survey students. See Appendix D for college web page URLs and addresses.

Case Review: Worcester Polytechnic Institute

Contact was initially established with WPI on April 15th, following the first survey request. Permission was granted to distribute the survey to a list populated with 100 e-mail addresses of randomly chosen students. Permission for distribution in the fall semester was obtained on September 13th, along with a list of 100 student e-mail addresses.

Case Review: Clark University

Contact could not be established with Clark University during the spring semester. Following changing the administrative contact within the college, contact was established on August 14th, at which time the administrative contact gave permission to distribute to 100 students in the beginning of the fall semester. The list of e-mail addresses was received on August 29th, along with an offer to provide more addresses as necessary.

Case Review: Illinois Institute of Technology

Contact could not be established with Illinois Institute of Technology during the spring semester. Pursuing various administrative contacts yielded no results. Contact was finally established on September 13th, following the letter requesting permission to distribute to students through an independently generated list of e-mails. At this point, the administrative contact indicated that the college would need permission from several other offices before authorizing distribution. All further attempts at correspondence with the administrative contact were not returned.

Case Review: University of Chicago

Contact could not be established with University of Chicago during the spring semester. Pursuing various administrative contacts yielded no results. Contact was finally established on September 1st, following the late August phone call. The administrative contact indicated that the college would be willing to participate pending further details about the project. Upon the college's receipt of the details requested, a request for the list was subsequently denied, stating that permission had not been granted. Upon further investigation, the administrative contact indicated that distributing student e-mail addresses was against the college's policy.

Case Review: Georgia Institute of Technology

Contact could not be established with Georgia Institute of Technology during the spring semester. An administrator was contacted on April 16th. The message was redirected to a different administrative contact. The original administrative contact claimed to not have the authority to approve or decline the request. The second indicated that the first administrative contact was, in fact, the appropriate person. The first maintained that he was not in a position to authorize the survey request, and directed it to a third administrative contact. Contact with the third administrator was established on September 13th, following the letter requesting permission to distribute to students through an independently generated list of e-mails.

The third administrator politely requested that our team cease to pursue this matter at Georgia Tech for three reasons. The first reason was that the college was already engaged in a number of survey processes in view of approaching regional re-accreditation. The second reason was that the college could not afford to divert staff resources to the instrumentation of this project. The third and final reason was that the request needed to be reviewed by the Georgia Tech Institutional Review Board for several weeks before granting permission, and the administrative contact was not willing to devote the time to submit the paperwork necessary and take responsibility for the timely review of this project.

Case Review: Emory University

Contact was established on April 16th, following the initial spring semester survey request. The administrative contact indicated that the college was considering participation and requested further information about the project and how the data would be used. On April 20th, the administrative contact offered to distribute the survey to students personally.

Upon requesting permission to distribute the survey to students in the beginning of the fall semester, the administrative contact stated that she was no longer employed at Emory University and indicated the appropriate administrative contact within the college. On August 16th, contact was established with the second administrative contact. The administrative contact stated that he needed to investigate whether the survey was appropriate. On September 7th, the administrative contact replied, asking if distribution could be postponed until October to avoid interference with the college's surveying of its own students. Attempts to contact the administrators in October were unsuccessful.

Case Review: Harvey Mudd College

Contact with HMC was established on May 14th following the second spring semester survey request. The administrative contact indicated that the student government felt the request was too late in the semester to receive any legitimate replies.
On September 10th, the administrative contact agreed to distribute the project survey to all HMC students through the use of a mailing list following the e-mail indicating a September 10th deadline.

Case Review: Pitzer College

Contact could not be established with Pitzer College until September 13th, following the letter requesting permission to distribute to students through an independently generated list of e-mails. The administrative contact indicated that Pitzer College was not interested in participating at this time.

As a special case involving WPI and Clark University, a request for 400 additional names was emailed to the administrators. This was due to the fact that the number of students polled at HMC was disproportionate to the number polled at WPI and Clark University and the fact that students from WPI and Clark University were underrepresented in the responses. WPI approved and delivered the 400 additional e-

mail addresses. Clark University, however, declined to give 400 more e-mail addresses despite originally indicating that the college would be willing to offer more names if necessary. See Appendix C for a copy of this letter.

Upon further examination of the colleges' policies and administrative responses, assessments can be made regarding the college's reasons for declining to participate. Several different problems were encountered while attempting to gain the permission from the administrators at non-cooperating colleges including bureaucracy, student surveying, and policy restrictions. At Illinois Institute of Technology, three independent offices were required to volunteer approval before such a survey could be distributed. At Georgia Institute of Technology, the administration was pressured by the accreditation board to survey their own students, which took precedence over the instrumentation of this project. Similarly, Emory University was also preoccupied with conducting surveys of its own. University of Chicago stated that supplying student e-mail addresses was strictly against the college's policy. Likewise, it can be inferred that all colleges might be resistant to mass-mailings or the supplying of student e-mail addresses due to college policy. Pitzer College provided no definitive reasons for not participating in this project.

VI. Data Analysis Methodology

The respondents' emails were placed into a single text file to allow for continuous parsing of survey data. A program developed in Microsoft Visual Basic 6.0 was implemented to extract the data from the bracketed fields in the e-mail-based replies. The data from each survey was stored as a record in a Jet SQL database for easy analysis and retrieval.

An e-mail header in the data file delimited each survey. The data for each question was determined by locating the start of the question and parsing out the known number of subsequent bracketed fields attributed with the given question. By maintaining a strict context in terms of the questions being presented in the data file, erroneous entries were properly handled. Open-ended questions were handled by extracted all lines following the question up to the start of the next question. To properly handle text-based numerical entries such as fractions and approximate figures such as "8-9", all entries were extracted as text strings and subsequently converted accordingly.

Storing the data into a Jet SQL database permitted extended analysis. Using Microsoft Access 2000, the data could be correlated, grouped, and sorted dynamically. SQL queries permitted selective retrieval and formatting of records, which could be entered into a Microsoft Excel 2000 spreadsheet for the purposes of graphing and continued analysis. This allowed for selecting the data grouped by various demographics and other correlating elements. Many types of graphs are possible using Microsoft Excel 2000's chart objects, which can represent data in a variety of useful ways depending on the context of the comparison.

VII. Survey Results and Data Analysis

This section is intended to provide an explanation of the data to be analyzed, an overview of that data and a question-by-question analysis of the survey results. The data was analyzed through various groupings of demographics such as school, class, and gender. The graphs are intended as a tool for visual comparison.

The data analyzed includes the survey results from HMC and WPI. The results from Clark were omitted as only four out of one hundred students polled completed the survey. Statistically, this data could not be used to infer any information about the Clark University population as a whole. This does, however, indicate that e-mail may be less effective at schools with a lesser technical focus.

HMC and WPI are both highly competitive engineering colleges. Without results from a liberal arts college, the analysis is limited in scope to the network behavior and policy effects of engineering colleges. The scope of this analysis is also limited in geography, as only two of the four geographic regions are represented. The reduction in variables between the two colleges limits the number of factors that could be responsible for differences within the data, allowing for more conclusive comparisons between the two colleges.

	HMC	WPI
Total	**717**	**2,817**
Men	**506**	**2,165**
Women	**211**	**652**
% Male	**70.6%**	**76.9%**
% Female	**29.4%**	**23.1%**
Students Polled	**717**	**500**
Students Responding	**58**	**41**
Men Responding	**40**	**28**
Women Responding	**18**	**13**
% Male Responding	**69.0%**	**68.3%**
% Female Responding	**31.0%**	**31.7%**
Freshmen Responding	**15**	**16**
Sophomores Responding	**17**	**7**
Juniors Responding	**12**	**6**
Seniors Responding	**13**	**11**

Figure 6-1: Breakdown of college population and respondents

As is common among engineering colleges[25], Figure 6-1 shows that there are significantly more men in attendance than women at each college. As all the students attending HMC were polled, and a true random sampling of WPI students were polled, the recipients were likely to be of the same male-female ratio as the colleges. With a disparity of gender response less than 10% in both schools, it is not clear that on gender would be any more or less likely to respond than the other.

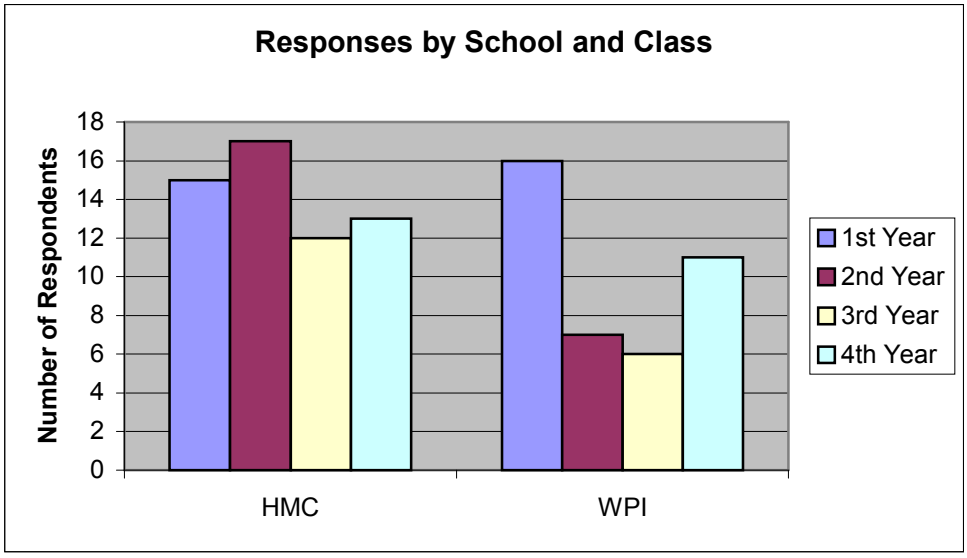

Figure 6-2

In Figure 6-2, there is a significant amount of variance shown in between the classes for WPI, which must be taken into account when examining other data grouped by class. The small percentage of returns may account for much of the differences in numbers of respondents between classes at each college, however other factors may include increasing freshman class sizes, retention rates, WPI undergraduate project programs, and the potentially higher interest of freshmen in the subject.

The following is a list of each question from the survey, followed by graphical representations and analysis of the data collected. The data is graphed by class, school, or gender in order to clearly highlight any differences and meaningfully represent the results.

```
1. In the brackets below, enter the average number of hours per day you
   spend accessing the Internet through:

[  ] Worcester Polytechnic Institute's Network
[  ] Home Connection
[  ] Workplace Facilities
[  ] Other
```

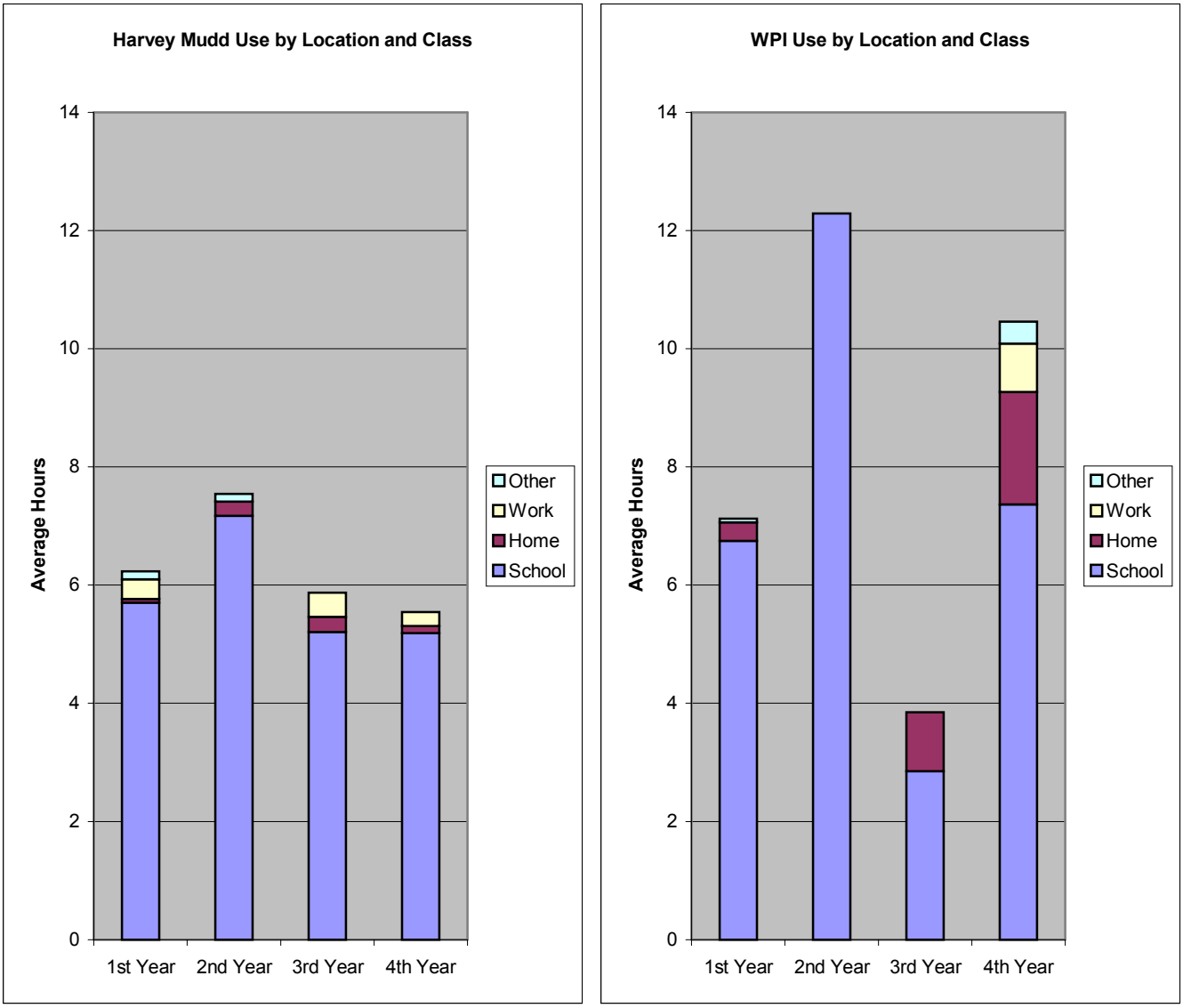

Figure 6-3: Use by Location and Class

Figure 6-3 shows that more WPI juniors and seniors use off-campus facilities to access the Internet than any other school-class grouping. The average of the total hours of use across the classes of HMC is constant. Much of the variance of the WPI data can be attributed to respondents claiming to personally access the Internet for 24 hours at a location. This is indicative of server use, which constitutes a computer running and being

connected to the network constantly. The question may have been clearer if the personal use had been stressed. While the scale changed, the WPI data maintained the same pattern upon removal of the 24-hour outliers.

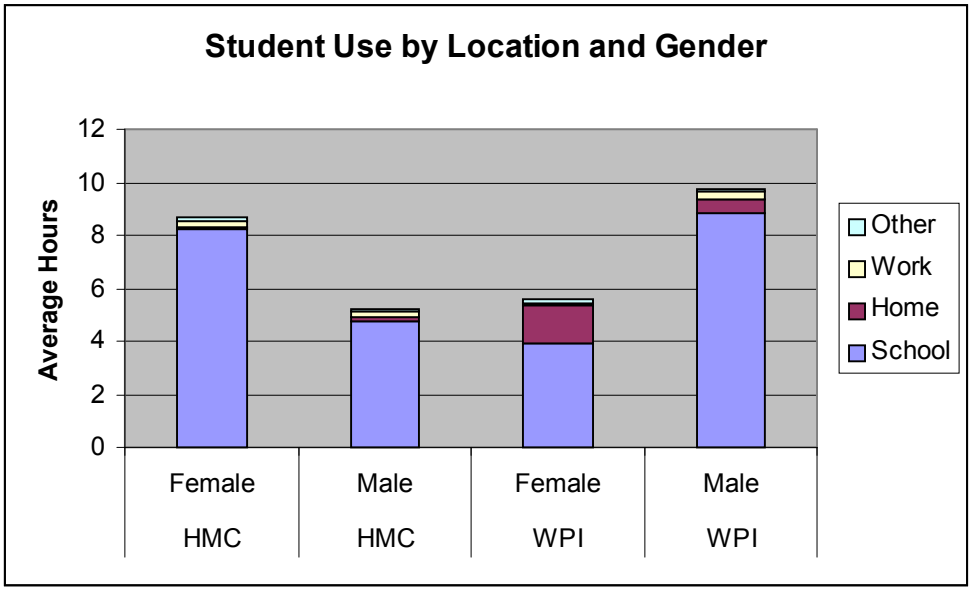

Figure 6-4

Figure 6-4 surprisingly indicates that while males at WPI access the Internet dramatically more than females, females at HMC access the Internet dramatically more than males. The data continued to support this conclusion when the 24-hour outliers were filtered. WPI females spend more time accessing the Internet from home than WPI males.

```
2. In the brackets below, enter the average number of hours per day you
   spend on each of the following activities:

[  ] Email
[  ] Other Internet Communication (e.g. Instant Messenging, Chat)
[  ] Academic Web Browsing
[  ] Shopping Online
[  ] Other Non-Academic Web Browsing
[  ] Downloading Music
[  ] Downloading Software
[  ] Downloading Other Media
[  ] Playing Network Games
[  ] Sharing Music
[  ] Sharing Software
[  ] Sharing Other Media
[  ] Hosting Network Games
[  ] Hosting Commercial Websites
[  ] Hosting Non-Commercial Websites
```

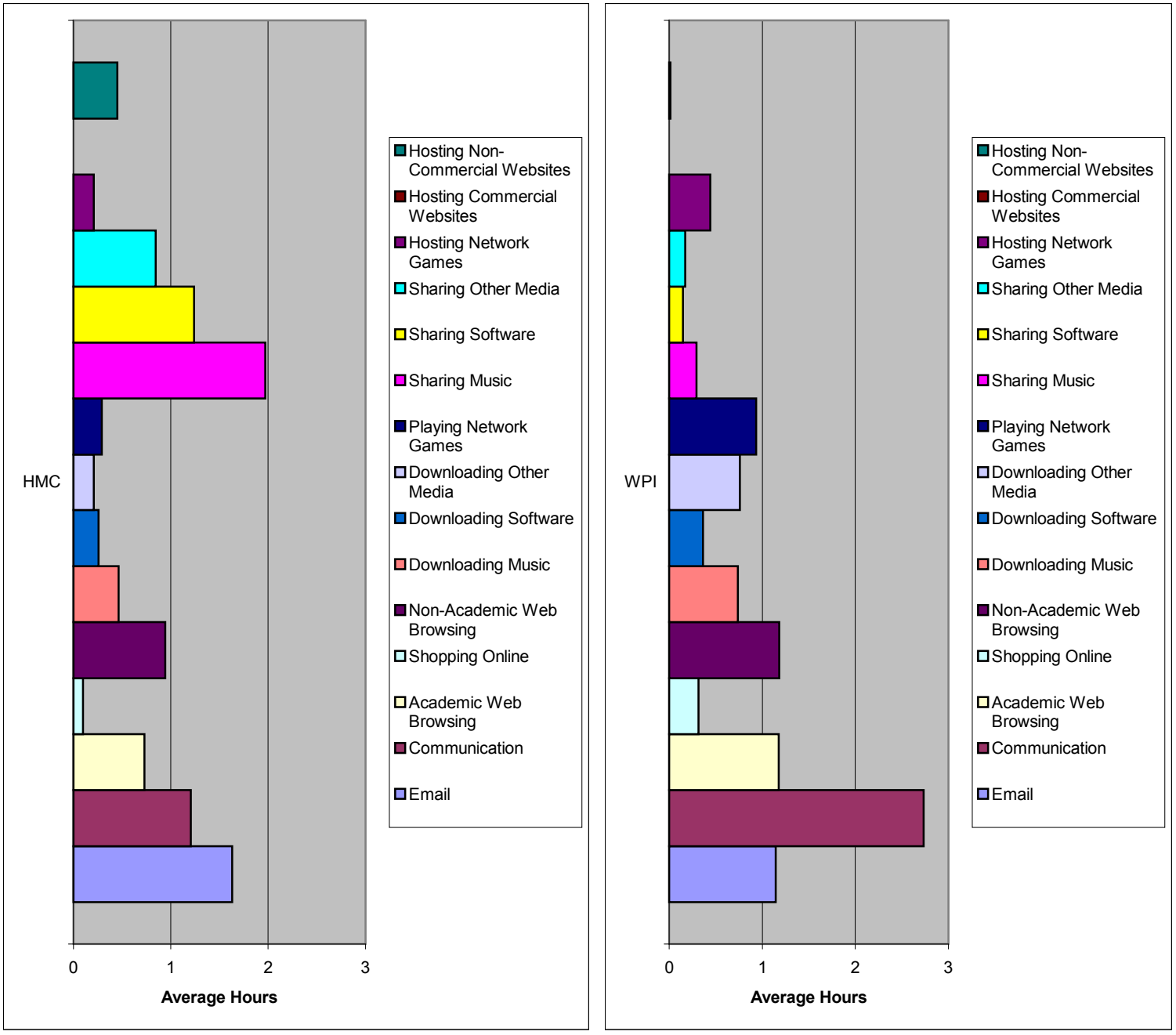

Figure 6-5: Network Use in Activities by School

There are several key differences depicted in Figure 6-5 between HMC's student network use and WPI's student network use. The first of these is that HMC's students in general spend much more time sharing music than WPI students. While both colleges prohibit the distribution of copyrighted material, the time spent sharing music and software at HMC was over 6-8 times higher than that of WPI.

Figure 6-5 also indicates that WPI students had 120% higher use of on-line communication such as instant messaging than HMC students. In turn, WPI students spend less time on e-mail. Use of instant messenger may have curtailed the use of e-mail at WPI as a more effective communications medium. Likewise, the on-line gaming community has a more significant presence at WPI. Non-commercial webhosting on personal computers seems more common at HMC, but this may be due to WPI's active support of non-commercial websites on college servers. The figure does not indicate any other significant difference in usage between the two colleges.

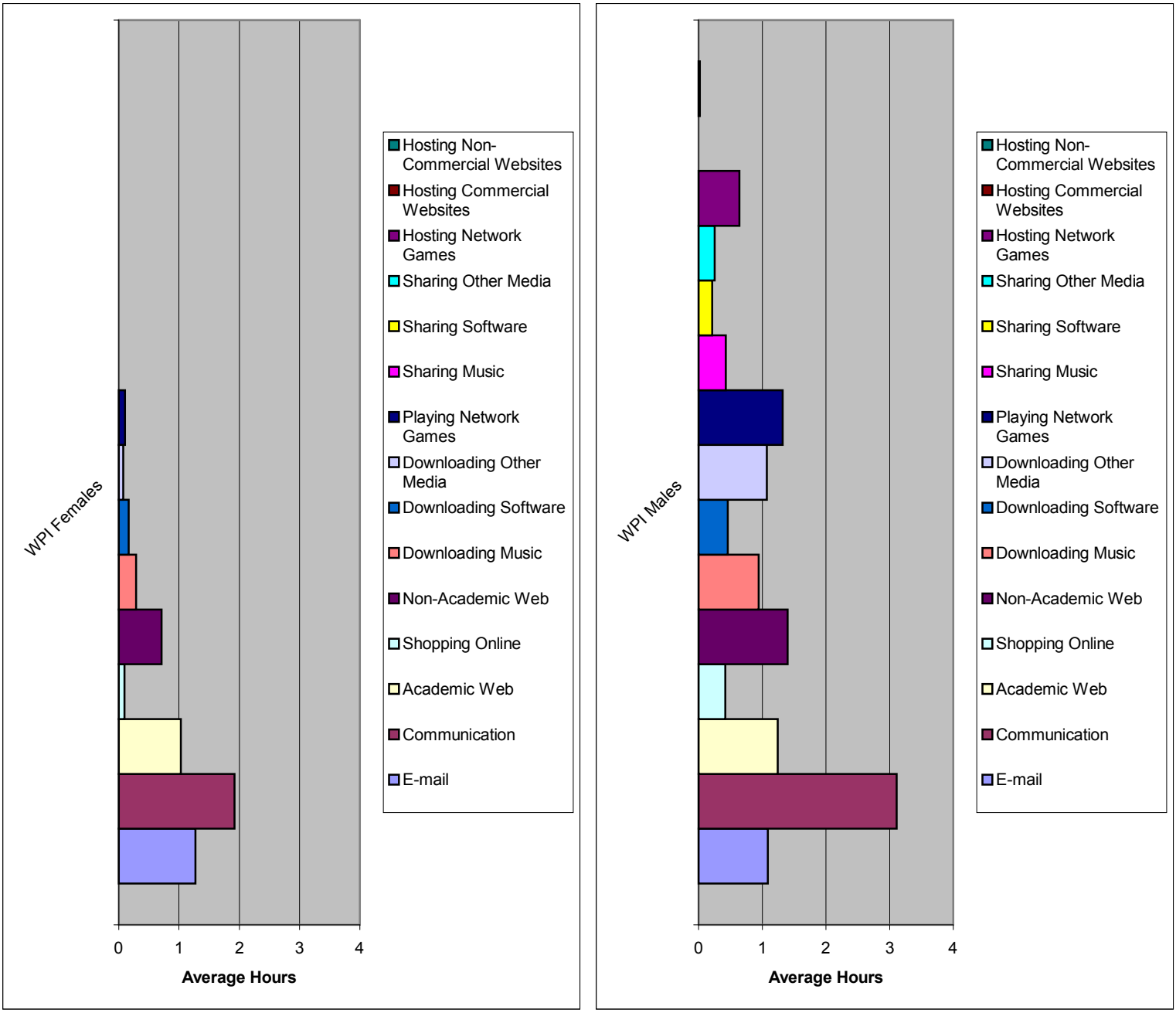

Figure 6-6: WPI Network Use in Activities by Gender

In Figure 6-6, we see that not only is the overall female network use lower at WPI with male use at 12.6 hours and female use at 5.6 hours, but the variety of activities as well. Females make up a disproportionately small portion of the gaming community, engage in less non-academic web browsing, and share virtually no media.

Academic web browsing, communication, and e-mail remain popular among both men and women. Nina K. Simon, an undergraduate at WPI who achieved the Society for

Women Engineers Award and the Gertrude R. Rugg Award for academic excellence among women in engineering and science was interviewed on the topic of network use disparity between men and women. She indicated that WPI females find the computer to be more of a computer tool than a recreational tool. This is the purported cause of smaller amount of file sharing and game playing among WPI females. She also indicated that WPI females are more involved in extra-curricular activities and clubs than males, which limits time spent on the computer.

Another possible basis for this difference is the disparity of gender among majors. Computer science majors may engage in a higher level of network use. A relatively small number of women participating in computer science would, in turn, decrease the average lower level of network use among women.

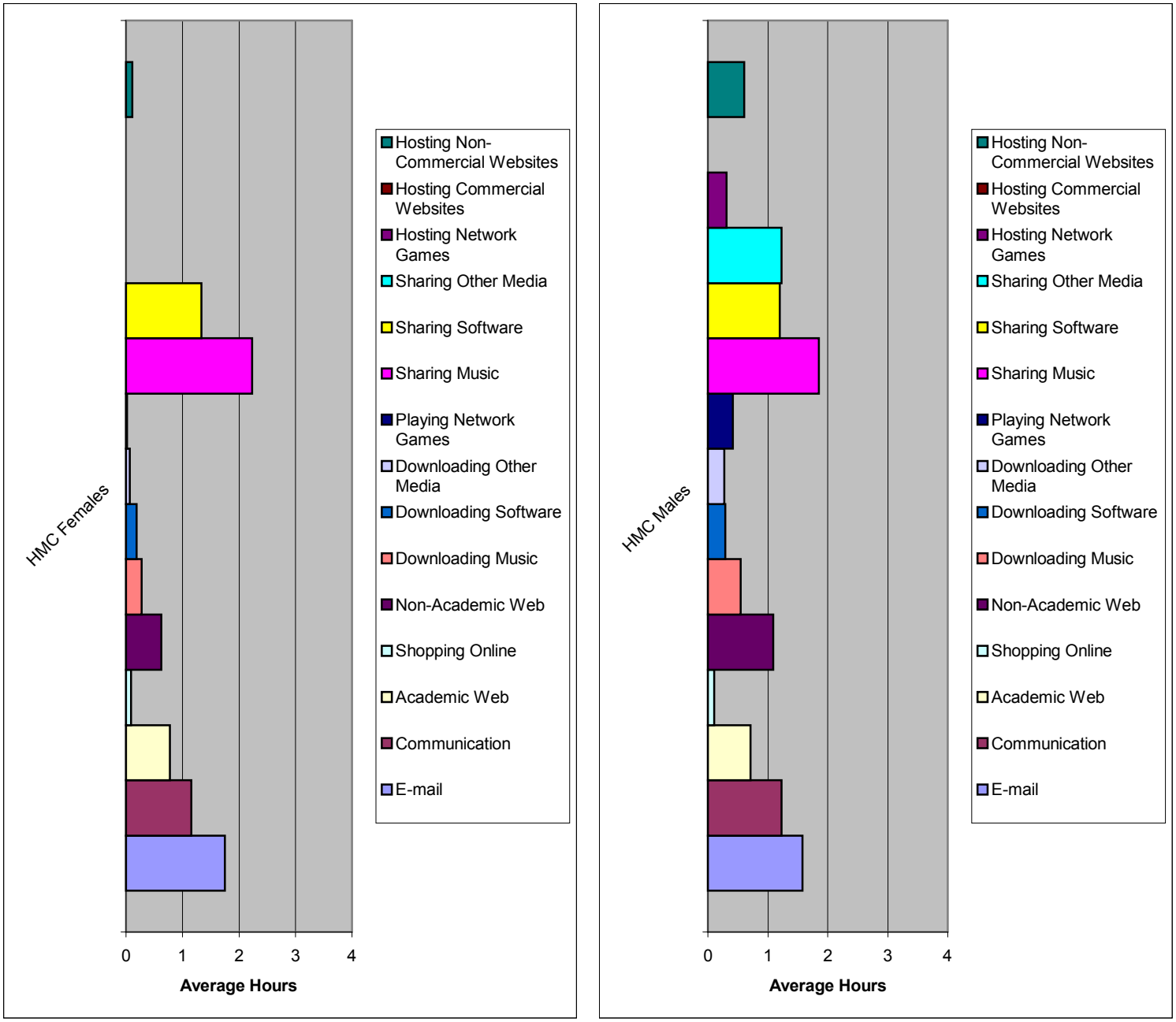

Figure 6-7: HMC Network Use in Activities by Gender

Figure 6-7 shows that there is more similarity in network use between males and females at HMC than WPI. Like WPI, few females at HMC are participants in the on-line gaming community. Non-academic web browsing is also less pronounced among females. Both sexes actively engage in media sharing.

A disparity exists between the overall network use indicated on Figure 6-7 and those indicated in Figure 6-4. Figure 6-7 indicates that males have a marginally higher overall use of the network, while Figure 6-4 indicates that female network use is significantly higher. Analysis of the two sets of data reveals that the female responses are more consistent, indicating that men either dramatically underestimated their total use or overestimated their specific activities. The former is more likely, as the activities portion of the survey forces the student to analyze his or her behavior more carefully.

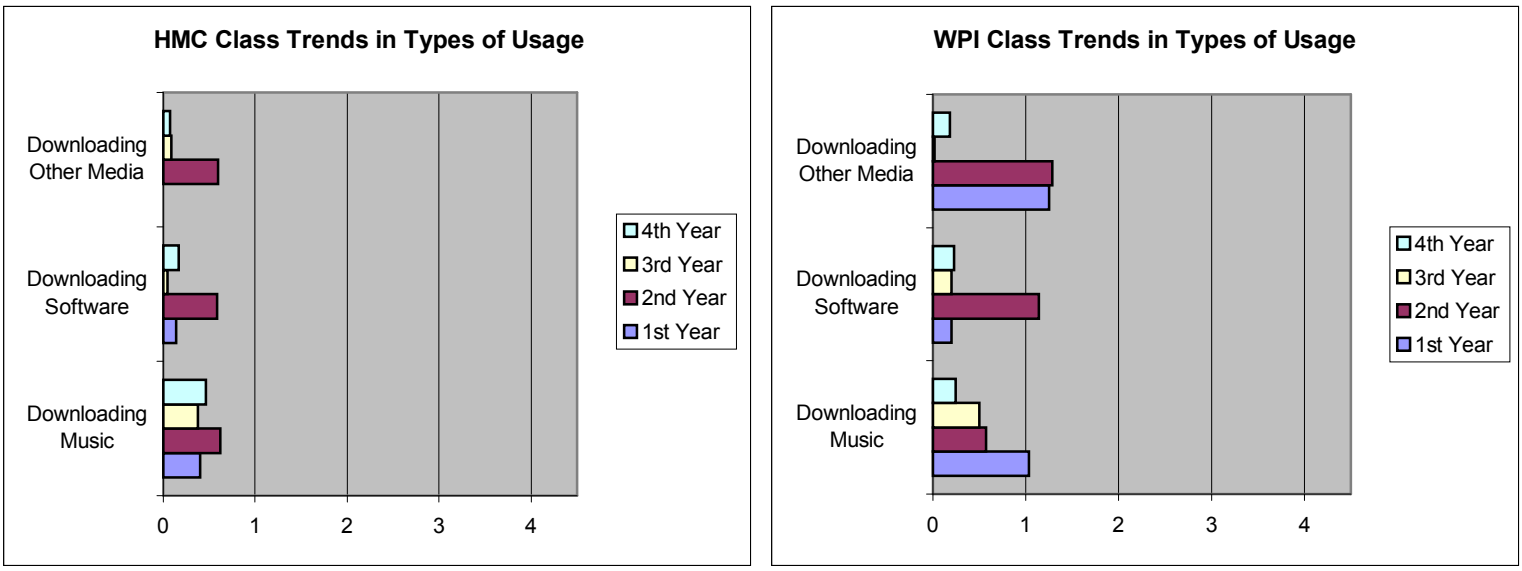

Figure 6-8

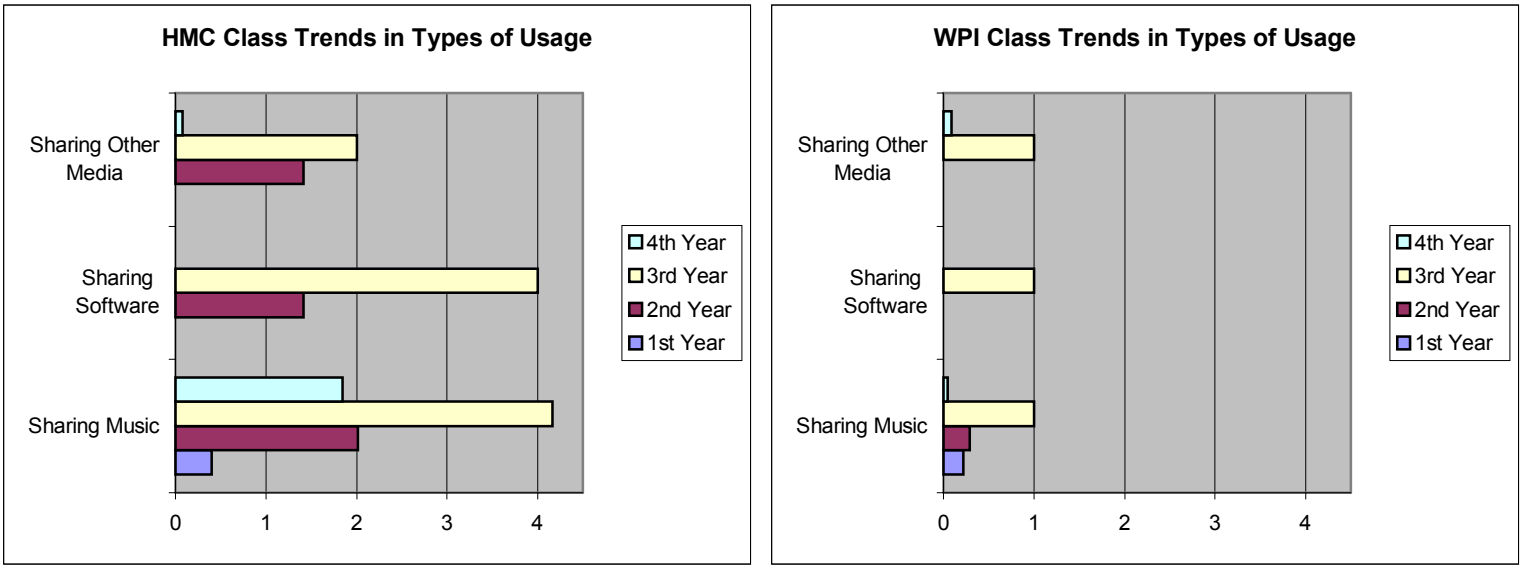

Figure 6-9

Figures 6-8 and 6-9 indicate a surprising relationship between sophomores and juniors of both colleges. At both WPI and HMC, the juniors are the greatest distributors of all three types of media, while the freshmen and sophomores are the greatest recipients of all three types of media despite the fact that both colleges' policies prohibit such activity.

```
3. Do you feel in any way limited in your self-expression or expression of
   opinion online (e.g. e-mail, web pages, online communication)?

[ ] Not Limited
[ ] Somewhat Limited
[ ] Limited
[ ] Severely Limited
```

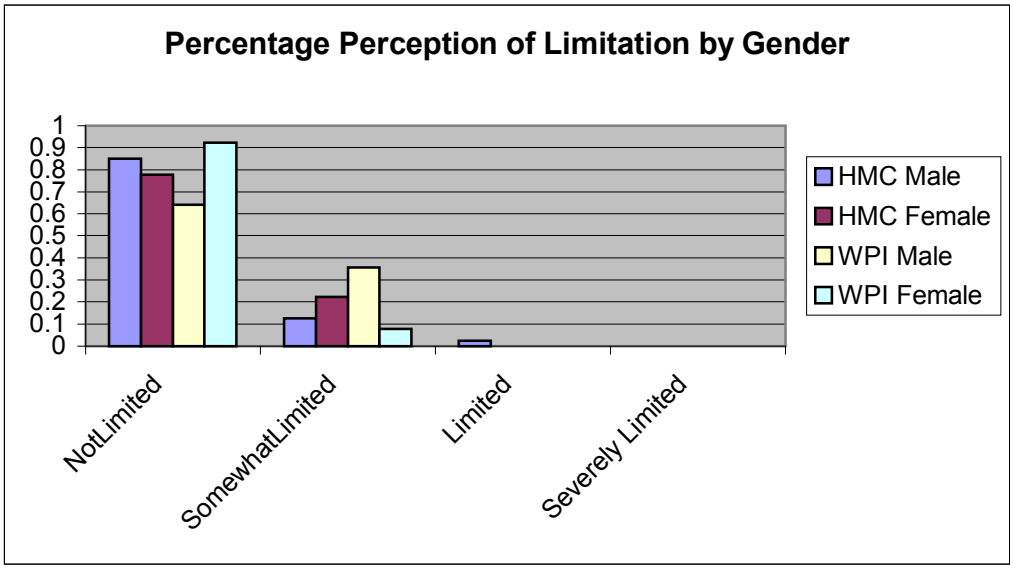

Figure 6-10

Figure 6-10 indicates that the vast majority of students at both colleges feel that they are in no way limited in their self-expression online. However, 80% fewer WPI females feel limited in their self-expression than males. The opposite, although to a lesser extent, is true at HMC.

Due to a potential greater interest in media sharing among males at WPI, males may feel more limited, as they are unable to share music and software with their friends without repercussion, although it is not clear whether WPI females largely abstain from media sharing due to lack of interest as opposed to policy. Also, males may be more inclined than females to participate in activities that may damage their reputation if

known of publicly, such as viewing pornography or general excessive use. The increased awareness of monitoring on the WPI campus network could make such habits seem less private and explain a greater sense of limitation.

```
4a. Are you comfortable with giving out private information over Worcester
    Polytechnic Institute's network (e.g. address, credit card numbers,
    social security numbers)?

[ ] Yes
[ ] No

4b. Are you comfortable with giving out personal information over Worcester
    Polytechnic Institute's network (e.g. medical history, legal records)?

[ ] Yes
[ ] No
```

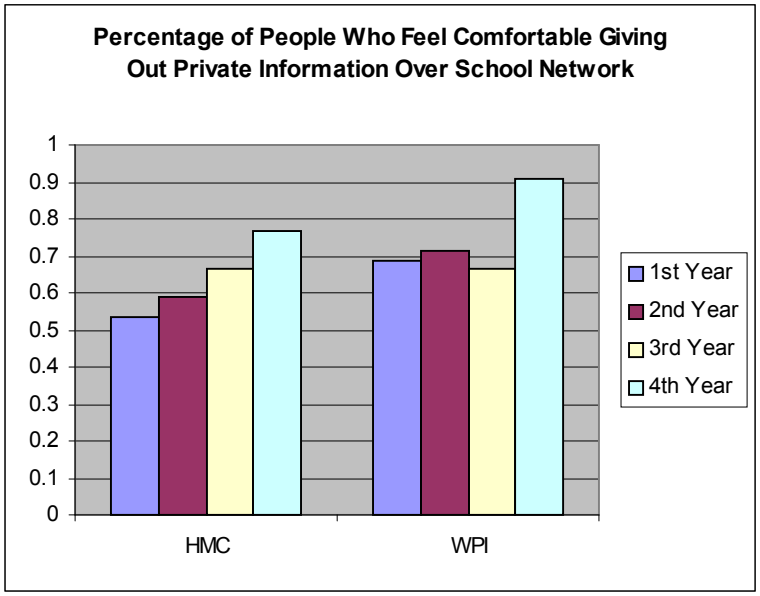

Figure 6-11a

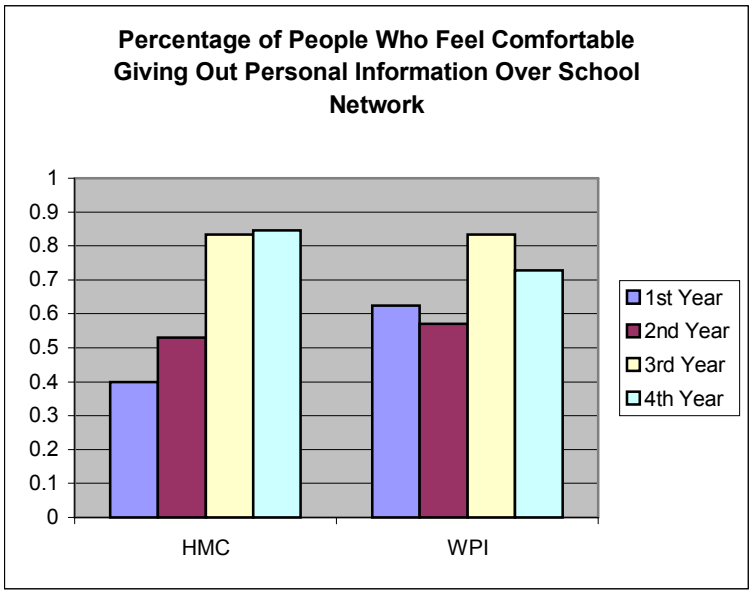

Figure 6-11b

Overall, in Figure 6-11a and 6-11b, the students at the respective colleges indicated little difference about whether they were comfortable in giving out private or personal information over their college's network. At HMC the indication of comfort increased with class year while no such trend was apparent in WPI's student body. WPI students indicated that they were more comfortable with giving out private information than personal information.

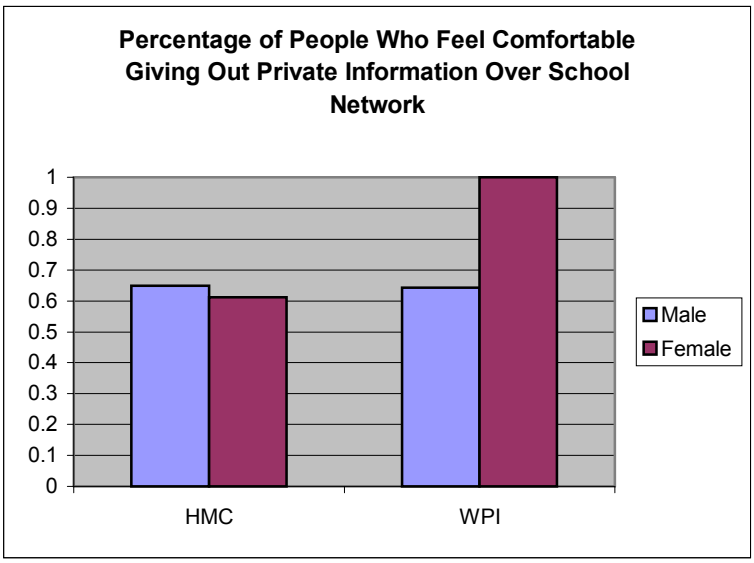

Figure 6-12a

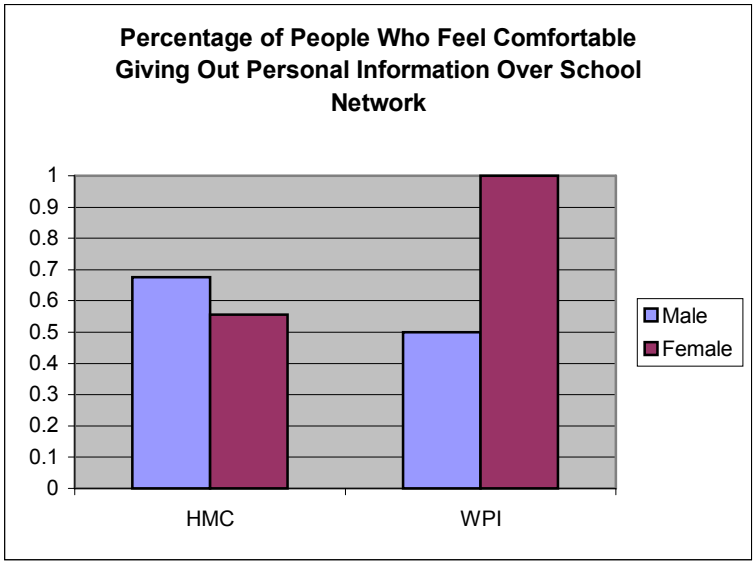

Figure 6-12b

Figures 6-12a and 6-12b indicates that females at WPI feel much more comfortable giving out personal and private information over the network than males. This correlates closely with Figure 6-10, wherein WPI females felt far less limited in their self-expression. This supports the conclusion that WPI males feel more limited because they are more concerned about their personal or private communications or activities being monitored. The females at HMC felt little different from males.

Most personal and private information is channeled over communication and non-academic web browsing. The lack of concern for personal or private data does not appear to have affected use in those areas positively, as the level of on-line communication such as e-mail and instant messaging is the same between males and females, while non-academic web browsing is actually less. On the other hand, it is possible that if females shared the same level of concern for privacy as males, female on-line communication may have been as low as other female activities in proportion to male use.

```
5. In what ways are you aware that Worcester Polytechnic Institute's
   Network Use Policy has been made available?  'X' all that apply.

[ ] Available paper copy (e.g. library)
[ ] Distributed paper copy (e.g. orientation)
[ ] Published on-line
[ ] Word of mouth
[ ] Not published
[ ] Other
    Please specify
    >
```

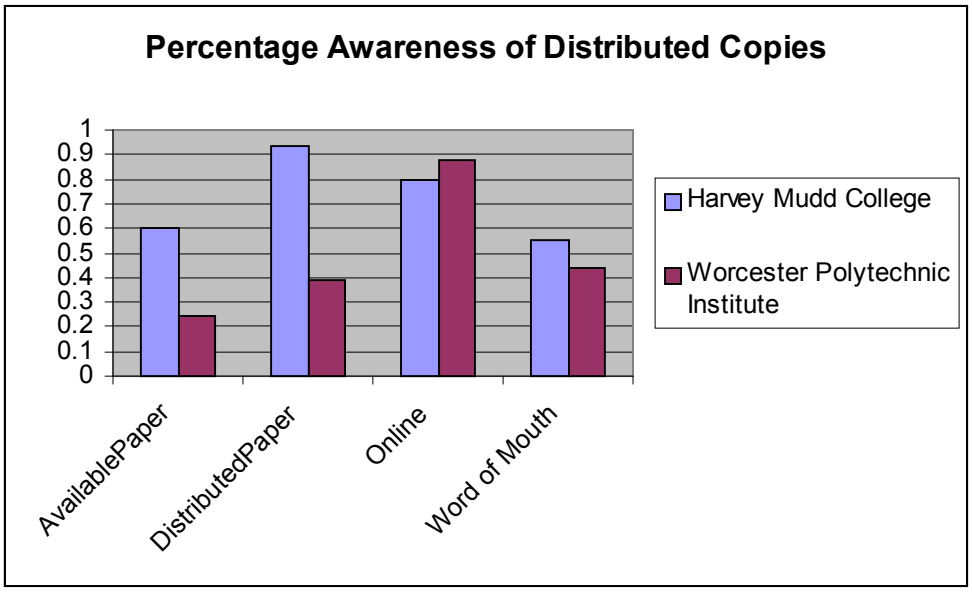

Figure 6-13

Figure 6-13 clearly shows some of the differences in how each college educates its students. Almost all HMC students are aware of the policy through a printed copy given to them by the administration, quite possibly during orientation. Most WPI students were either not given such a copy or do not recall receiving it. WPI's library has printed copies of its network use policy available, but that is not immediately obvious to the uninitiated. Any number of means is possible to generate awareness of policies at the library, including a rack of college handouts at checkout, clear signage, and explicit indication at orientation. Both colleges make it easy to find the policy on-line.

```
6. Indicate your familiarity with Worcester Polytechnic Institute's
   published Network Use Policy?

[ ] Completely unfamiliar
[ ] Somewhat unfamiliar
[ ] Somewhat familiar
[ ] Very familiar
```

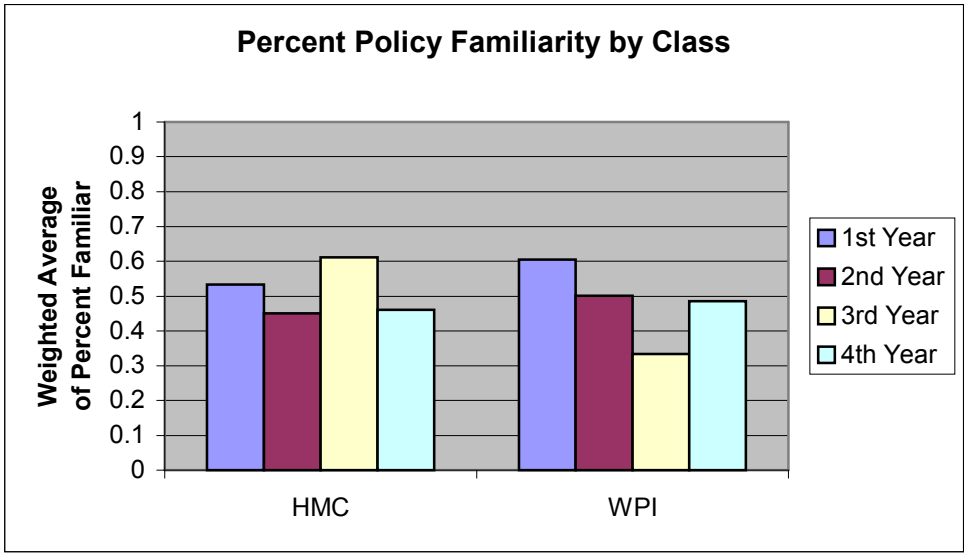

Figure 6-14

Figure 6-14 averages the results on a scale from 0 – Completely Unfamiliar to 1 – Very Familiar. Familiarity of the policy among students neither significantly increases nor significantly decreases with class year. There is also little difference between the two schools, overall.

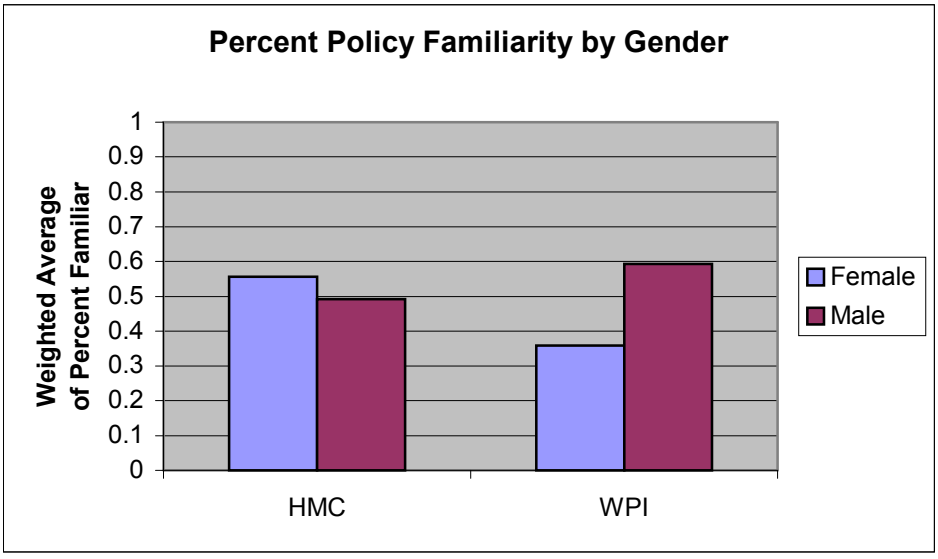

Figure 6-15

Figure 6-15 shows that WPI females are significantly less familiar with the network use policies. This could be due to the lack of female use of file sharing services.

Since the policy is less likely to affect them, they have less reason for being familiar with the policy's terms.

	HMC	WPI
Total Familiar	52	33
Total Unfamiliar	6	7
Females Familiar	15	8
Females Unfamiliar	3	5
Males Familiar	37	25
Males Unfamiliar	3	2

Figure 6-16: Breakdown of Students
by Selection of "Completely Unfamiliar"

Many students indicated a small amount of familiarity, but only 10% declared themselves completely unfamiliar. As a result, the sample size and the sampling itself were not heavily altered for questions #7-9, which require some familiarity of the policy.

```
7. For each of the following, type an 'X' in the box that indicates whether
   there are actively enforced restrictions placed on each activity on
   Worcester Polytechnic Institute's network.


Yes No  Unknown

[ ] [ ] [ ]    Email
[ ] [ ] [ ]    Other Internet Communication (e.g. Instant Messenging, Chat)
[ ] [ ] [ ]    Academic Web Browsing
[ ] [ ] [ ]    Shopping Online
[ ] [ ] [ ]    Other Non-Academic Web Browsing
[ ] [ ] [ ]    Downloading Music
[ ] [ ] [ ]    Downloading Software
[ ] [ ] [ ]    Downloading Other Media
[ ] [ ] [ ]    Playing Network Games
[ ] [ ] [ ]    Sharing Music
[ ] [ ] [ ]    Sharing Software
[ ] [ ] [ ]    Sharing Other Media
[ ] [ ] [ ]    Hosting Network Games
[ ] [ ] [ ]    Hosting Commercial Websites
[ ] [ ] [ ]    Hosting Non-Commercial Websites
```

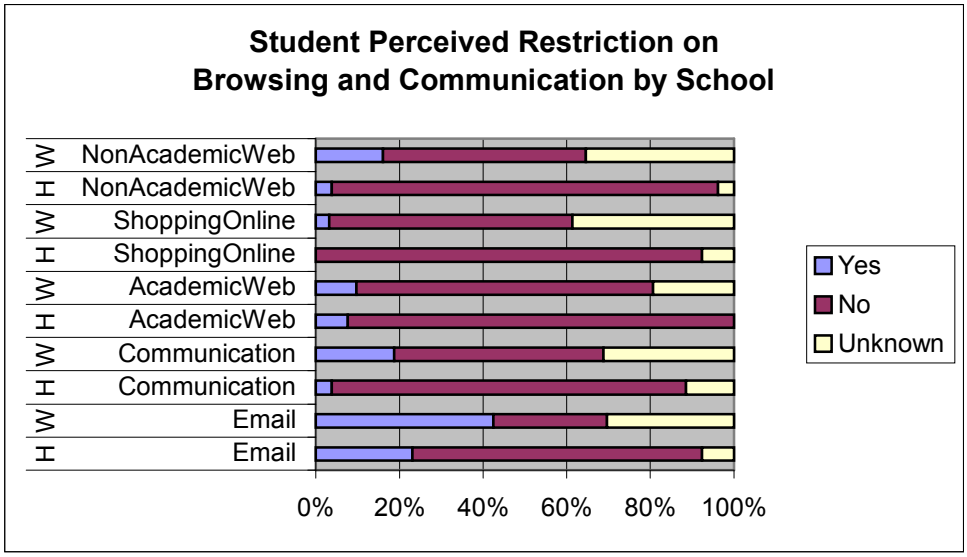

Figure 6-17

Figure 6-17 reveals several details about student perceptions at either college. In all cases, more WPI students perceive restrictions on browsing and communication than HMC students. A significant number of students in both colleges perceive restrictions on the use of e-mail. It is not clear whether this indicates simple administrative restrictions, such as abuse of mass-mailing lists, or whether it indicates a sense of limitation in what can be said over e-mail. For both colleges, the percentage of students indicating that they perceive enforced restrictions on e-mail is similar to the percentage of students who indicated some limitation in self-expression, lending credence to the latter possibility.

Uncertainty as to enforcement is significantly higher among WPI students than it is among HMC students. In question #9, four students from HMC referred to a college policy known as the Honor Code. One student spoke of the nature of the Honor Code, stating, "You can do as you wish as long as you do not break laws or dishonor the school or yourself." He goes on to say that students are trusted as long as they prove to be untrustworthy. If such a code were to supercede the policy in practice and were well known, that would explain such differences seen above.

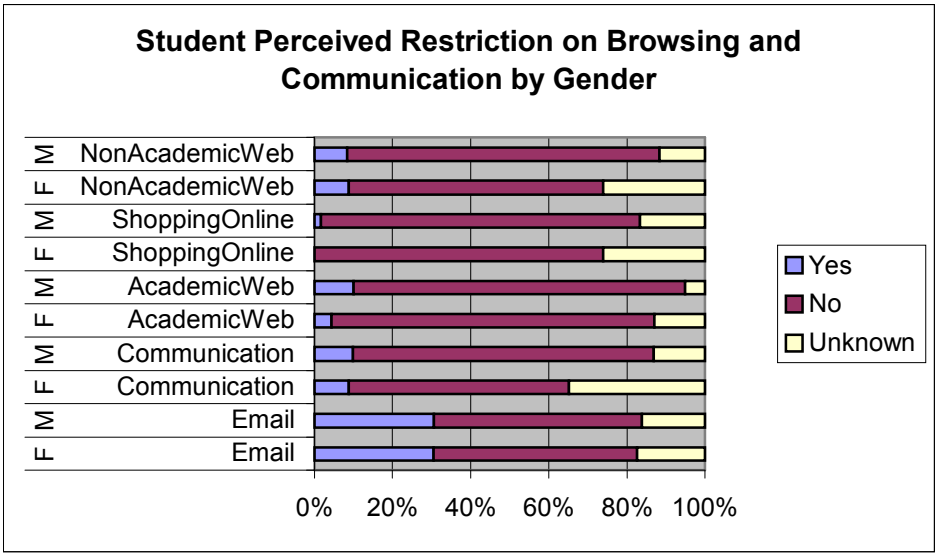

Figure 6-18

In order to successfully group the results into men and women and draw meaningful conclusions about each general gender differences without weighting by school, the proportions of males to females responding between HMC and WPI would have to be similar. The proportion of males to females in HMC responses is 2.5, while the proportion of males to females in WPI responses is 3.1. In extreme cases, this can misrepresent gender by up to 11%, while the misrepresentation will be significantly less in typical cases.

Figure 6-18 indicates that both men and women feel equally restricted in the area of browsing and communication.

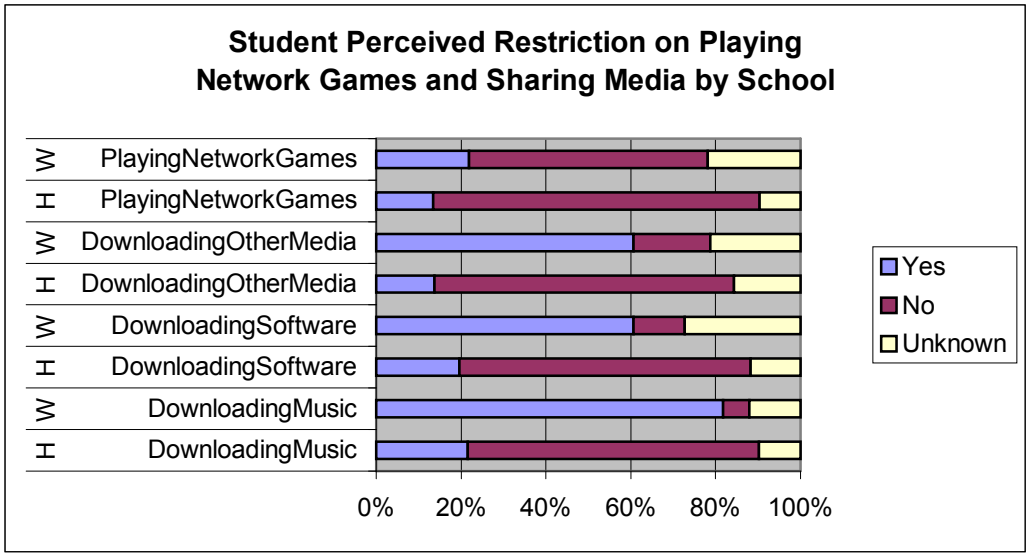

Figure 6-19

Similar to Figure 6-17, Figure 6-19 indicates that more WPI students perceive restriction or are uncertain than HMC students. When it comes to sharing media, the difference between WPI students and HMC students is dramatic, despite the fact that the colleges have similar policies. The discrepancy is at least partly due to the fact that WPI has engaged in campus wide enforced restrictions while HMC's Honor Code implies that students are to be dealt with on a person-by-person basis.

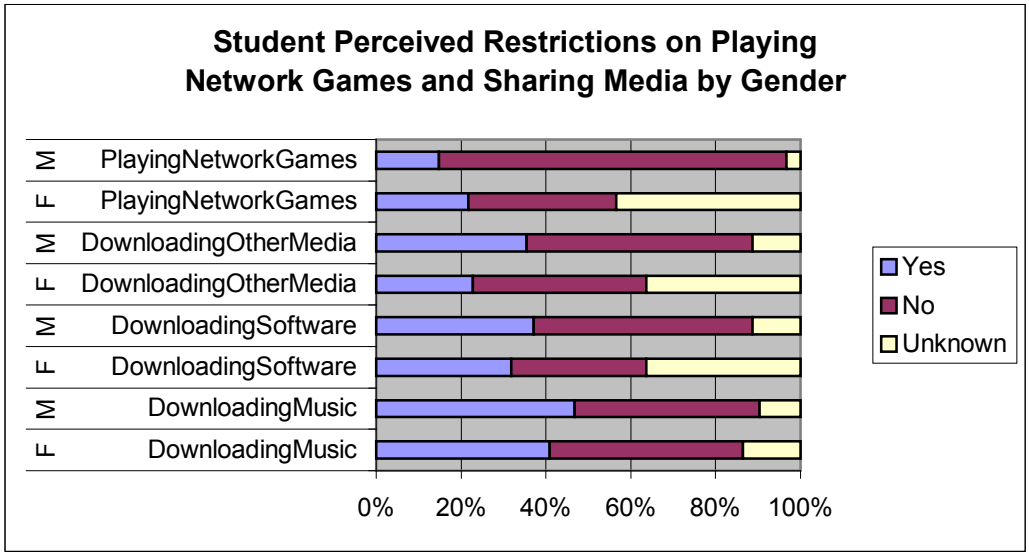

Figure 6-20

In Figure 6-20, several differences are apparent between the sexes. Males largely dominate on-line gaming; hence the perception of restriction among females is largely unknown. Less than 20% of men are aware of any enforced restrictions on on-line gaming.

The downloading of other software and other non-music media is less common among females in both colleges. The lack of such activity among females seems to be the primary cause of unfamiliarity with the restrictions in that activity.

Downloading music is highly popular among both males and females in general. Such use is equivalent among both males and females at HMC, while at WPI, males download music more, but only marginally. As expected, the equivalency of use correlates to an equivalency of perception on restriction.

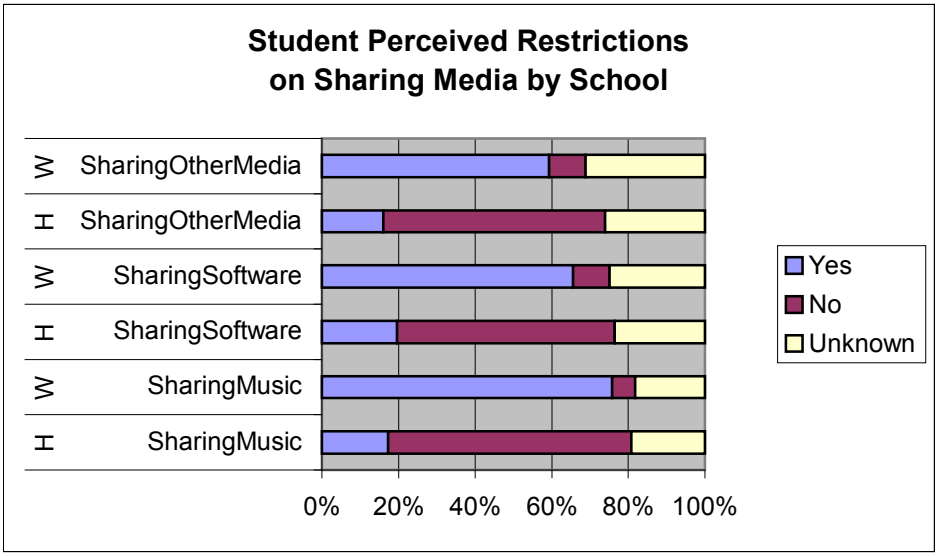

Figure 6-21

The perceived restriction of media sharing in Figure 6-21 closely parallels that of media downloading in Figure 6-19. The results are tied directly to a difference in enforcement.

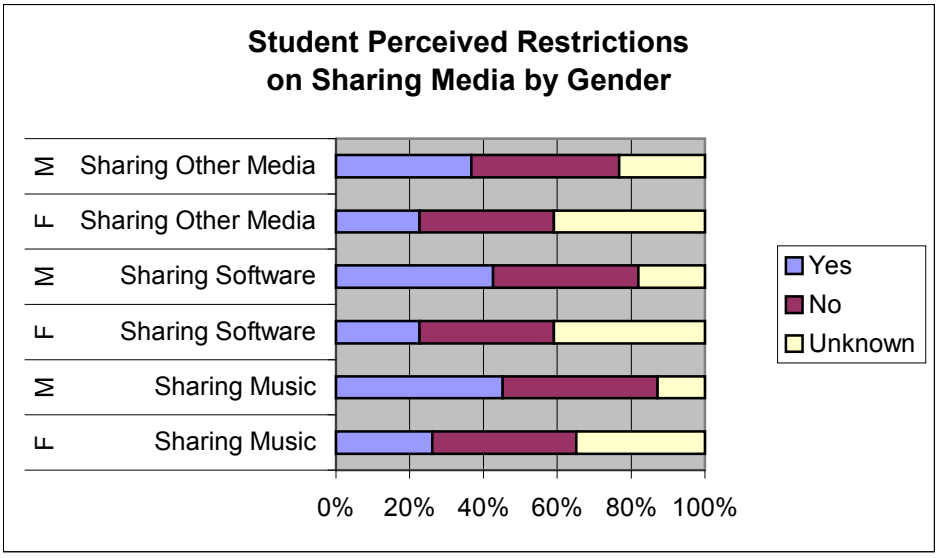

Figure 6-22

In all cases, the number of people who perceive restrictions is the same as the number of people who do not. Females are less certain in all three areas, which does not directly parallel use. One possible explanation is that while the time spent by females on media sharing is not especially different from that of men, they participate more casually. A second possibility is that a male-dominated staff of network administrators is less likely to impose restrictions on females than males, and as a result, fewer females hear about instances of imposed restrictions first-hand.

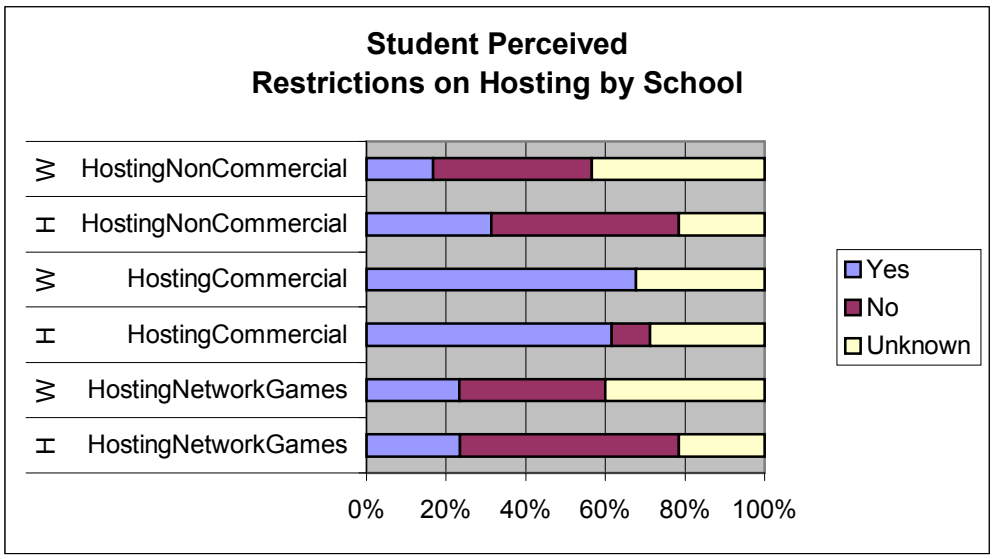

Figure 6-23

Non-commercial web hosting is one of the few categories perceived as being less restricted at WPI compared to HMC. This is likely due to WPI's encouraging students to create web sites on the college's public servers. It follows that if hosting a web site with college resources is acceptable, that hosting a web site with personal resources is equally acceptable. Commercial websites are unquestionably untolerated. Despite WPI's considerable gaming community, Figure 6-23 indicates that they feel no less restricted than HMC students.

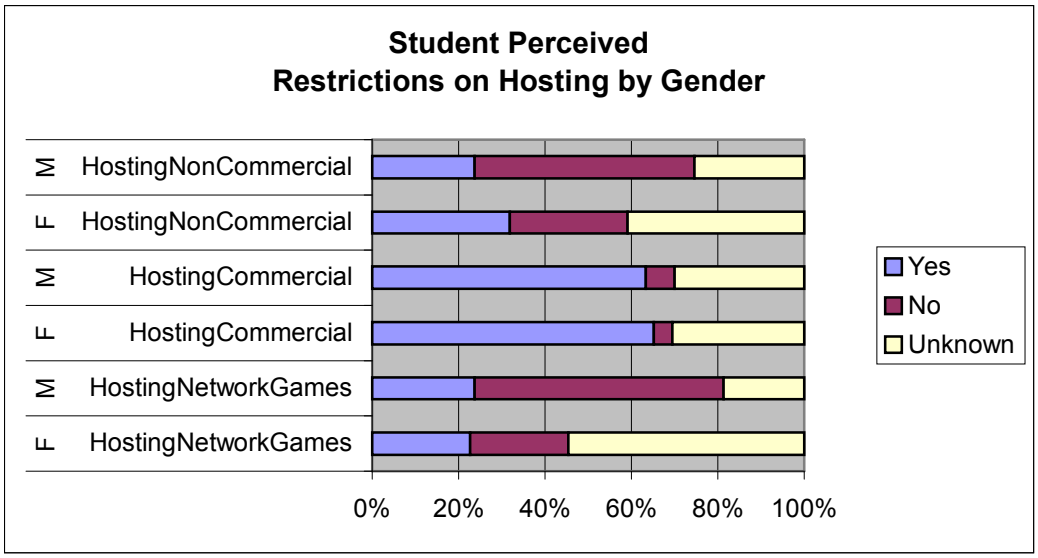

Figure 6-24

According to a recent Netcraft survey[26], the use of Linux with Apache is the most popular combination for personal web hosting. Linux and its popular suites of applications are developed under the Free Software movement and the Open Source movement, both of which are heavily dominated by males[25]. The increased uncertainty and sense of restriction among females as shown in Figure 6-24 is a likely consequence of that domination. Similar is the hosting of network games, another area that is heavily dominated by males.

```
8. How would you rate Worcester Polytechnic Institute's Network Use Policy?

[ ] Lenient
[ ] Somewhat lenient
[ ] Neutral
[ ] Somewhat strict
[ ] Strict
```

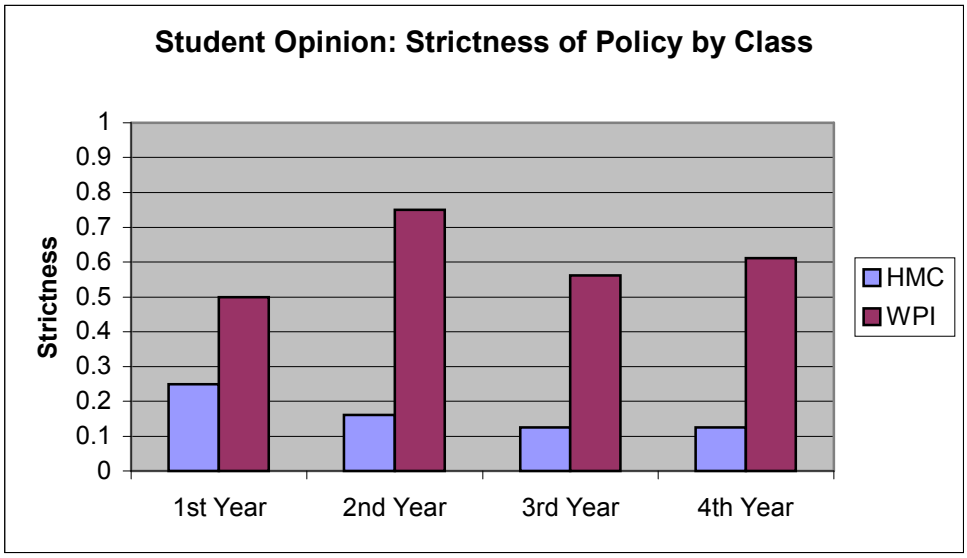

Figure 6-25

Figure 6-25 averages the results on a scale from 0 – Lenient to 1 – Strict. The survey was distributed shortly after the start of classes, which would indicate that freshman responses are based on first impressions. HMC's indication of strictness is low, and in fact decreases with each class, showing that the leniency exceeds initial expectations. WPI's indication of strictness increases after freshman year. Within a month of using the campus network, students at WPI have a much greater impression of policy strictness than students at HMC, and that gap widens with experience. Judging from the similarity in policies between the two schools as well as the students' similar levels of familiarity with the policy, the gap must be due to methods of enforcement.

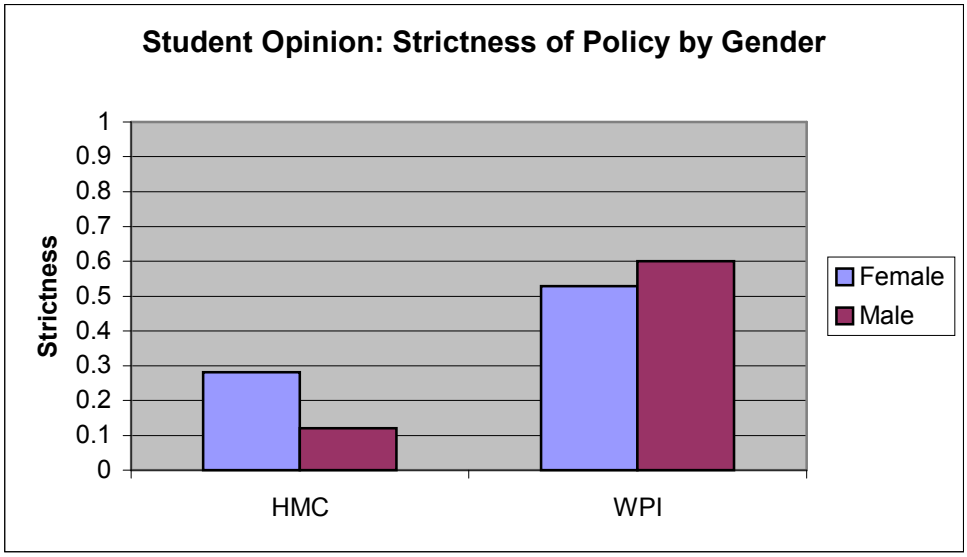

Figure 6-26

Figure 6-26 indicates that males and females at WPI find the strictness of policy to be almost equally high. At HMC, however, females feel that the policy is almost three times stricter than males do. This may be related to females' increased use of computer networks at HMC, as shown in Figure 6-4.

```
9a. I feel Worcester Polytechnic Institute's Network Use Policy is:

[ ] Unfair
[ ] Somewhat unfair
[ ] Neutral
[ ] Somewhat fair
[ ] Very fair

9b. Briefly express the reasons for your choice in 9a.
>
>
```

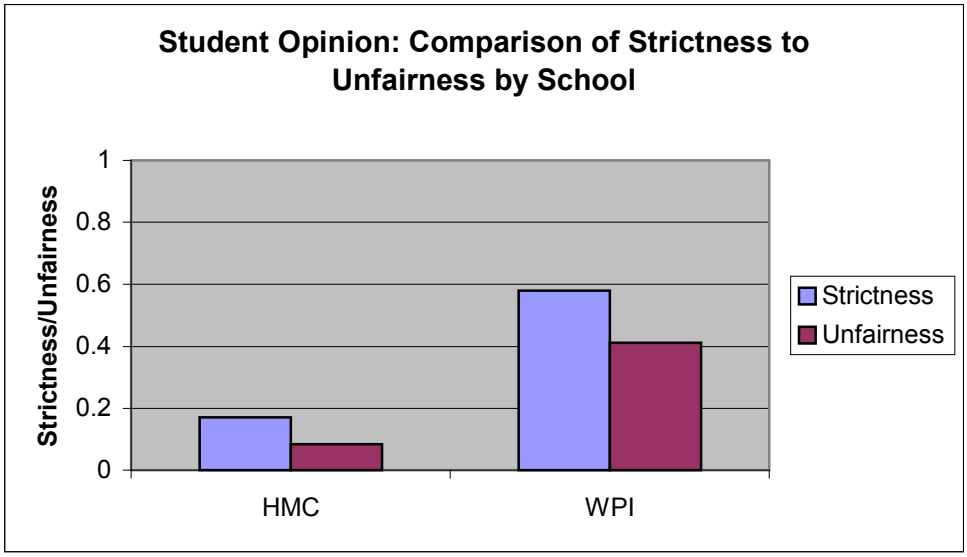

Figure 6-27

Figure 6-27 includes the results from both question #8 and question #9 for comparison, averaging the results on a scale from 0 – Fair to 1 – Unfair and from 0 – Lenient to 1 – Strict. Students may deem strictness in a policy to be a necessary fact of life, and hence determine it to be fair. Many students who found WPI's policy to be somewhat strict indicated the answers "Neutral" or "Somewhat fair." The same phenomenon can be seen at HMC on a smaller scale.

Still, overall WPI students find their policy to be much less fair than that of HMC, indicating that many feel the strictness to be unwarranted.

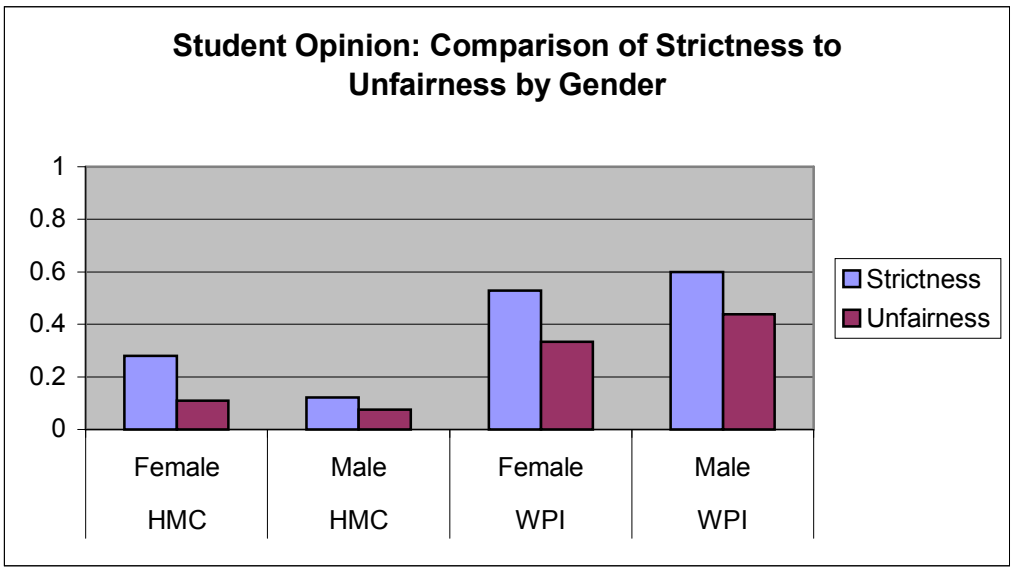

Figure 6-28

The behavior observed above exists for all genders. The most dramatic difference is that of HMC females who generally feel that their policy is only somewhat lenient, while finding their policy to be very fair. Similar to trends seen elsewhere in this analysis, males at WPI feel the policy to be significantly stricter than females.

```
10. How would you rate Worcester Polytechnic Institute's overall
    enforcement of the Network Use Policy?

[ ] Not enforced
[ ] Lightly enforced
[ ] Neutrally enforced
[ ] Heavily enforced
[ ] I do not know
```

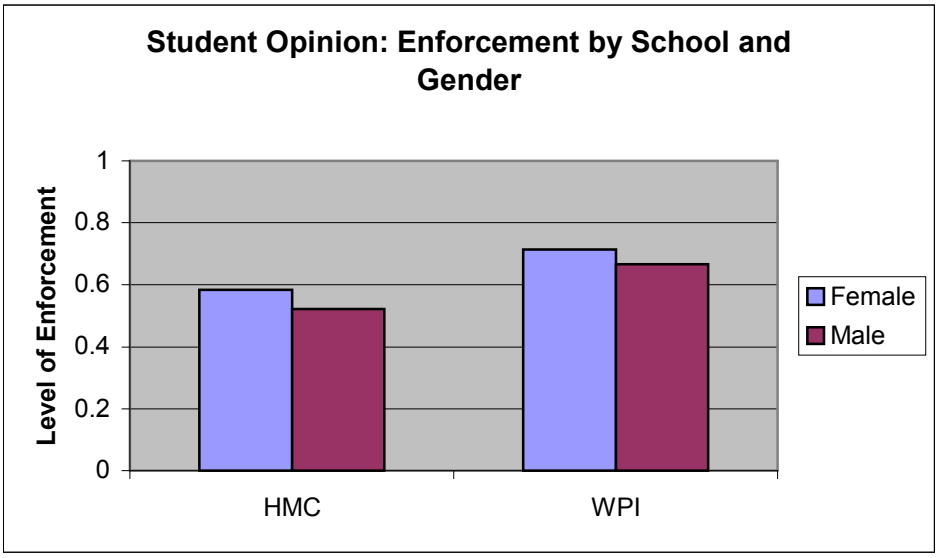

Figure 6-29

Figure 6-29 averages the results on a scale from 0 – Not Enforced to 1 – Heavily Enforced. In contrast to previous trends, Figure 6-29 indicates that the females at WPI indicated an equal or greater enforcement of policy than males. Females may put more emphasis on enforcement protecting them from third parties, which could make them more comfortable sharing personal or private information as indicated in Figure 6-12a and Figure 6-12b. Alternatively, with increased and more prohibited use of the network, males may have a better sense of what is and is not enforced.

Interestingly, HMC students feel their policy to be nearly as well enforced as WPI students do, despite the dramatic difference in reduced active restrictions indicated in the figures related to question #7.

```
11. Briefly express the most obvious way the Network Use Policy has
    affected your use of the network, if at all.
>
>

Any other comments you wish to make about Worcester Polytechnic Institute's
Network Use Policy:
>
>
```

	HMC	WPI
No Effect	18	3
Blank	20	13
Feel More Secure	2	1
Better Network	2	0
Academic Inconvenience	2	2
File Sharing	9	20
E-Mail	1	0
Games	1	1
Web Hosting	2	0
Not Certain	1	1

Figure 6-30: A Tally of Student Responses to Question #11:
The Most Obvious Impacts of Network Use Policy

Question #11 allowed us to examine types of use that may have been overlooked. By going through the answers, all of the most obvious effects of the network use policy could be properly categorized and tallied.

After a survey forcing many students to analyze their restrictions, many students at HMC say they feel completely unaffected by the policy. In fact, a few feel that their network is actually better due to the policy. One student submitted the following commentary:

> It's lenient and fair. They protect the interests of the students while not limiting our online options. We also have wireless networking, free printing, multiple free labs, free wireless-enabled laptops available for checkout. They run excellent and well-administered services (finger, pop, ftp mirrors, proxy, dhcp, firewall imap, free http and ftp accounts for each student) - they allow us to have multiple ports per student and several static IPs per student (important for running servers). All in all, HMC networking is the best I've ever seen or heard of…

Some students in both schools indicated that various automated restrictions related to limiting file sharing applications actually prevented them from working on

projects. A WPI student pointed out, “Some programs they block serve academic and non-violating purposes as well.” This most likely alludes to file sharing programs like Gnutella, under which not all media is copyrighted and some is viable for academic use. Another WPI student complained, “We pay a fortune and certain web sites are blocked off!!!” which likely includes Audio Galaxy, a popular web-based music sharing application. Another WPI student made the point, “As long as you are not doing anything illegal, offensive or taking up more than your share of the bandwidth they let you use what they have.” This coincides with our interview of WPI administration who stated that excessive use of bandwidth was the primary reason for shutting down file-sharing services. A fourth WPI student had a different take on the matter, stating, “It is fair in every way that is necessary for WPI to support copyright protection, and work to prevent offensive material from reaching personal web pages hosted by WPI.”

One WPI student indicated that the college protected him from legal action. When an organization like the Recording Industry Association of America asks for information about alleged copyright violators, the college will not supply it without a subpoena. A college like Harvard University where such legal issues are left to user discretion is far less likely to involve itself in a dispute between students and third parties.

The thinking of HMC students runs along similar themes, but with a different perspective. “It [The policy] seems pretty fair, in that they put academic priorities first, i.e., limiting bandwidth to other uses.” Another student cites the honor code. “The honor code makes it based on your own integrity, so it's completely fair.” A more cynical student wrote, “You could practically get away with murder...”

One HMC student refers to an abandoned effort to sponsor free and open communication through e-mail through anonymity. “Great freedom is granted in allowing students use of network resources so long as excessive (many gigabytes) bandwidth is not used up in the process. However, the college as an academic institution should encourage political freedoms where possible, yet the idea to run an anonymous email node was immediately viewed with great fear and squashed.” It is possible that such administrator inhibitions account for the sense of restriction on communication at HMC.

VIII. Conclusions

This section details the conclusions drawn from the data collection process and the data analysis of the survey results. While the data analysis highlights the major conclusions of this project, administrative reaction to our requests was somewhat revealing of attitudes and motivations. The analysis has created a fairly comprehensive picture of the effects of varying perceptions of enforcement, as well as perspective differences between genders and academic classes.

Without community awareness and student interest, administrative contacts have little motivation to grant permission aside from good will and possible interest in good intercollegiate relations. In fact, without adequate student representation to affirm interest, there is the fear that permission may backlash on account of student complaints. Furthermore, administrative contacts may not trust the authors of the project to handle the data in a non-abusive fashion. A very significant factor was the amount of administrative effort involved in approving our request. This is evidenced by the number of responses we received after we offered to independently generate the distribution list.

Naturally, WPI accepted the request for students, as it has a history of actively supporting the qualifying projects of its student body. While Clark University's assistance is not to be taken for granted, they have close ties to WPI and have a long history of student-based research, particularly in the field of psychology. HMC's matter of acceptance is interesting. In other colleges, the decision of whether or not to permit the distribution of the survey lied in the hands of one or more key faculty members. Contrastingly, HMC left the decision with an academic board comprised largely of students. By having the students directly involved in external affairs, HMC achieves a higher level of community representation.

In conclusion, a lack of correspondence with a student body can result in a college being closed off to possibilities which students might otherwise take interest in. Through a lack of student representation, colleges may avoid activities, organizations, and opportunities that students would otherwise take interest in, preventing the academic community from reaching its full potential.

Due to the limited number of colleges participating or otherwise not giving adequate response, this project could not achieve two of its goals. One goal this project failed to achieve was the determination of differences in student behavior and policy between liberal arts colleges and engineering colleges. While Emory University opted to participate in the spring and Clark University opted to participate in the fall, both were too underrepresented to provide any analysis with respect to that goal. The lack of responses from liberal arts colleges indicates that e-mail surveys may be more effective in technology-oriented colleges. The second goal this project failed to achieve was the determination of differences between separate regions in the United States. In order to establish a norm for any one region, more than one college is necessary. Likewise, only two regions were represented.

The colleges analyzed were both competitive engineering colleges in liberal regions of the nation with similar network use policies. This makes the result set very practical for achieve the project's more concrete goals of comparing the colleges in terms of its enforcement, and any differences or lack of equitability between sexes and among the four undergraduate classes.

The gender differences in network use were far greater at WPI than those at HMC. Traditionally, males have largely dominated the extended use of computers. According to Nina K. Simon, females at WPI find using the computer for recreational use to be "frustrating." It is not entirely clear why the gender gap is much smaller at HMC than at WPI. One hypothesis supported by the data is that a lesser level of restriction on HMC students makes them feel more free to experiment with new aspects of computer and network use, resulting in more equitable experience between genders than experienced previous to attendance at HMC. Another hypothesis is that the socio-political climate in HMC's region may be more favorable to equity between genders than that of WPI's region.

After being forced to contemplate their individual activities, males recorded a greater level of network use than that recorded in question #1 of the survey. Judging from this, males have a tendency to underestimate their overall network use. Many male students may be surprised to discover how much time they really spend on-line. Females at WPI are more likely to spend time on extra-curricular activities and clubs than males.

If this sociological behavior is also prevalent at HMC, this may account for the gender gaps in the levels of network use at HMC as well as WPI.

Females at WPI feel much more comfortable giving out personal and private information over the network than men. This increased comfort in sharing may be caused in part by the higher presence of administration on the network at WPI compared to HMC. WPI females may feel that a responsible administration can protect their information from being monitored or abused by fellow students. Another potential factor is the decreased use of the network by females at WPI, which could correlate with ignorance of the potential for privacy violation, as evidenced by females' lower familiarity with the policy.

The data clearly indicates that the level of enforcement used at WPI is effective at maintaining the policy goal of prohibiting the illegal distribution of copyrighted material. The maintenance of this policy is actually a secondary goal to administrators at WPI, who are more concerned with keeping bandwidth available for academic use.

Almost every student at WPI who uses their computer at any length will experience the effects of network administration. Many file-sharing services are simply denied to all students. At HMC, students are far less likely to experience the effects of network administration, as students are dealt with on a case-by-case basis. This is more likely to happen for less severe cases, as offenders may be accused of breaking the HMC's Honor Code, which can have continuing repercussions. Interestingly, despite the frequency at which HMC students feel the effect of their policies, they are far more certain of which areas are restricted and which are not. A small set of straightforward principles such as the Honor Code is far more likely to generate awareness than a long list of rules and regulations.

From WPI’s case is reached the conclusion that while students may find a policy to be somewhat strict, they may also feel the policy to be fair overall. Student comments indicated that many students consider the limitations to be a necessary fact of life, barring other means to resolve the issues.

The level that students feel limited in their expression on the network correlates closely with how comfortable a student is giving private or personal information out over the network. Active monitoring of student use, or alternately ignorance about how a

network is monitored may result in students feeling that their privacy has been invaded, and hence may alter their on-line habits and communication as a result.

Some students at WPI indicated that prohibitions on file sharing limited their academic abilities. File sharing utilities provide a medium for the dissemination of all kinds of content, including academic content. For example, much genetic research has been published on Gnutella in an effort to make that research as widely available as possible. Colleges like WPI may need to go after individual offenders as HMC does rather than blocking whole services if they wish students to take advantage of the increasing non-violating uses of such services, although this opens up the potential for greater network abuse.

IX. Future Work

The insights gleaned from this project can be used to help develop the means and ideas necessary to help achieve the goals sought in future work. Such improvements on the project may include a broader range of test cases, improved methods of acquiring students' e-mail addresses, and more concise questioning on particularly interesting or surprising trends.

A broader range of test cases could be achieved by dividing the country into more than just four geographic regions. This would produce more data useful for analysis and determining trends based on location and socio-political background. A broader range of test cases on a local scale such as just within one local state may also produce pertinent data with respect to usage trends and comparisons within the immediate region.

Noting the difficulty in obtaining permission to distribute email surveys to students, a method of producing a higher acceptance rate would need to be established. However, it may prove difficult to establish another means of obtaining a random sampling of college students at a particular college. One possibility may be to go through campus organizations. Another possibility would be posting to the request in a frequented on-line forum in which such a request would be on-topic.

Other survey approaches may also be warranted. This is especially something to keep in mind given that far fewer students in liberal arts colleges responded to the e-mail surveys than students from engineering colleges. Getting permission to deliver a series of surveys to campus mailboxes with prepaid return postage may be effective, but it would be prohibitively expensive. An alternate approach would be to create a web-based form, and providing a few students financial incentive to print up promotional flyers directing students to the site and tack these fliers up around campus. By limiting the scope to local colleges, each campus can be visited and polled individually. This would eliminate problems with distance, and remove some of the focus from regional differences to differences between types of colleges, policies, networks, and enforcement.

After completing this survey process and analyzing the results, several interesting results emerged, such as significant gender gaps in the type of and quantity of time spent on network activities, as well as the greater role of enforcement and student perception

over actual policy. The reasons for these trends are not always evident as there may be several factors involved. More concise surveying on these topics may shed light on the reasons for these trends and explain why they exist even if they are not directly related to college policy. One such an interesting topic to survey would be discovering how, precisely, these modern file sharing services are put to use. Interesting trends are to be expected in the coming years as to how these new channels of distribution will be put to use. The results of this survey have placed an interesting perspective on gender roles in network use. Further study of these differences, as well as student opinion research as to how to approach the greater equity (if desired) should also prove fruitful. Targeting majors among the list of demographics would determine which types of students are the most deeply impacted, as well as helping to discern the differences in activities between majors.

Appendix A: Interview Questions

What do you feel are your major responsibilities in monitoring traffic?
What are the implementations in place to enforce policy?
What kind of penalties do you invoke for policy infringement?
Do you find that there is any student resistance to your policy?
Speaking generally, does your policy lean more towards a conservative or liberal viewpoint?
Do you feel your policy has strict terms in comparison with the policies of other colleges?
Do you find students tend to use the network more for internal or external uses?
Are there any community hotspots, if you will, on your network? Online forums where students congregate and share ideas?
What are the primary issues behind the existing policy? Is bandwidth a major concern? How do you handle issues of legality?
Do you find that any academic uses that are dissuaded?

Appendix B: Sample Survey

University Network Use Policy Survey

As part of our Interactive Qualifying Project at Worcester Polytechnic Institute of Worcester, Massachusetts, we are conducting a survey to collect information on effects and perceptions of network use policy. We would like to ask you to participate and help us with this project. The information submitted will be used for statistical purposes only. If you are interested in helping with this project, please complete the following using the directions provided and return the survey to usepolicy@wpi.edu in 72 hours.

In the following survey, type an 'X' within each of set of brackets corresponding to the most accurate option unless otherwise specified. (e.g. [X]) This survey will take 5-7 minutes to complete.

Demographic Information

School:

[ ] Harvey Mudd College (Claremont, CA)
[ ] Pitzer College (Claremont, CA)
[ ] Emory University (Atlanta, GA)
[ ] Georgia Institute of Technology (Atlanta, GA)
[ ] Illinois Institute of Technology (Chicago, IL)
[ ] University of Chicago (Chicago, IL)
[ ] Clark University (Worcester, MA)
[ ] Worcester Polytechnic Institute (Worcester, MA)
[ ] Other, please specify:

Gender:

[ ] Male
[ ] Female

Class:

[ ] 1st year student
[ ] 2nd year student
[ ] 3rd year student
[ ] 4th year student
[ ] Other

Network Use Policy Survey

1. In the brackets below, enter the average number of hours per day you

spend accessing the Internet through:

[ ] Worcester Polytechnic Institute's Network
[ ] Home Connection
[ ] Workplace Facilities
[ ] Other

2. In the brackets below, enter the average number of hours per day you spend on each of the following activities:

[ ] Email
[ ] Other Internet Communication (e.g. Instant Messenging, Chat)
[ ] Academic Web Browsing
[ ] Shopping Online
[ ] Other Non-Academic Web Browsing
[ ] Downloading Music
[ ] Downloading Software
[ ] Downloading Other Media
[ ] Playing Network Games
[ ] Sharing Music
[ ] Sharing Software
[ ] Sharing Other Media
[ ] Hosting Network Games
[ ] Hosting Commercial Websites
[ ] Hosting Non-Commercial Websites

3. Do you feel in any way limited in your self-expression or expression of opinion online (e.g. e-mail, web pages, online communication)?

[ ] Not Limited
[ ] Somewhat Limited
[ ] Limited
[ ] Severely Limited

4a. Are you comfortable with giving out private information over Worcester Polytechnic Institute's network (e.g. address, credit card numbers, social security numbers)?

[ ] Yes
[ ] No

4b. Are you comfortable with giving out personal information over Worcester Polytechnic Institute's network (e.g. medical history, legal records)?

[ ] Yes
[ ] No

5. In what ways are you aware that Worcester Polytechnic Institute's Network Use Policy has been made available? 'X' all that apply.

[ ] Available paper copy (e.g. library)
[ ] Distributed paper copy (e.g. orientation)
[ ] Published on-line
[ ] Word of mouth
[ ] Not published
[ ] Other
    Please specify
    >

6. Indicate your familiarity with Worcester Polytechnic Institute's published Network Use Policy?

[ ] Completely unfamiliar
[ ] Somewhat unfamiliar
[ ] Somewhat familiar
[ ] Very familiar

Skip questions [7-9] if you answered "Completely unfamiliar" to question 6.

---

7. For each of the following, type an 'X' in the box that indicates whether
   there are actively enforced restrictions placed on each activity on Worcester Polytechnic Institute's network.

Yes	No	Unknown	
[ ]	[ ]	[ ]	Email
[ ]	[ ]	[ ]	Other Internet Communication (e.g. Instant Messenging, Chat)
[ ]	[ ]	[ ]	Academic Web Browsing
[ ]	[ ]	[ ]	Shopping Online
[ ]	[ ]	[ ]	Other Non-Academic Web Browsing
[ ]	[ ]	[ ]	Downloading Music
[ ]	[ ]	[ ]	Downloading Software
[ ]	[ ]	[ ]	Downloading Other Media
[ ]	[ ]	[ ]	Playing Network Games
[ ]	[ ]	[ ]	Sharing Music
[ ]	[ ]	[ ]	Sharing Software
[ ]	[ ]	[ ]	Sharing Other Media
[ ]	[ ]	[ ]	Hosting Network Games
[ ]	[ ]	[ ]	Hosting Commercial Websites
[ ]	[ ]	[ ]	Hosting Non-Commercial Websites

8. How would you rate Worcester Polytechnic Institute's Network Use Policy?

[ ] Lenient
[ ] Somewhat lenient

[ ] Neutral
[ ] Somewhat strict
[ ] Strict

9a. I feel Worcester Polytechnic Institute's Network Use Policy is:

[ ] Unfair
[ ] Somewhat unfair
[ ] Neutral
[ ] Somewhat fair
[ ] Very fair

9b. Briefly express the reasons for your choice in 9a.
>
>

---

10. How would you rate Worcester Polytechnic Institute's overall
    enforcement of the Network Use Policy?

[ ] Not enforced
[ ] Lightly enforced
[ ] Neutrally enforced
[ ] Heavily enforced
[ ] I do not know

11. Briefly express the most obvious way the Network Use Policy has
    affected your use of the network, if at all.
>
>
>

Any other comments you wish to make about Worcester Polytechnic
Institute's
Network Use Policy:
>
>
>
>
>
>

Thank you for taking the time to participate in this survey.

Project Team:
 Adam Joseph Augusta   (roxton@wpi.edu)
 Michael Allan Narris (mnarris@wpi.edu)

Project Advisors:
 Mark Claypool, Assistant Professor   (claypool@wpi.edu)
 Robert Kinicki, Associate Professor (rek@wpi.edu)

Special Thanks to:
James Doyle, Associate Professor (doyle@wpi.edu)
Allan E. Johannesen (aej@wpi.edu)
Director of Internetworking, WPI
Sean M. O'Connor (soconnor@wpi.edu)
Network Manager, WPI

Appendix C: Form Letters

April 14th, 2001

To Whom It May Concern:

As part of our Interactive Qualifying Project at Worcester Polytechnic Institute of Worcester, Massachusetts, we are conducting a 5-7 minute survey to collect information on the effect and student perception of network use policy. Your college was one of eight selected in a case study of United States colleges with similar characteristics.

We request permission to deploy the following e-mail survey to a portion of [College]'s undergraduate students. If you and your school would be willing to participate in this survey, we would require at least 100 randomly selected undergraduate student e-mail addresses.

Please send an address list or an e-mail alias to usepolicy@wpi.edu. The contact information and the data collected will be held strictly anonymous and will be used for academic purposes only.

If you have any concerns, you may opt to personally distribute the survey electronically within the school. If you choose to do so, please notify us prior to its release.

For more information regarding our project, please visit the following URL: http://www.wpi.edu/~roxton/IQP/ProjectInfo.html

We encourage you to participate in the survey as well.

Thank you for your time.

Sincerely,
Adam Joseph Augusta (roxton@wpi.edu)
Michael Allan Narris (mnarris@wpi.edu)

Project Advisors:
Mark Claypool, Assistant Professor (claypool@wpi.edu)
Robert Kinicki, Associate Professor (rek@wpi.edu)

Special Thanks to:
James Doyle, Associate Professor (doyle@wpi.edu)
Allan E. Johannesen (aej@wpi.edu)
Director of Internetworking, WPI
Sean M. O'Connor (soconnor@wpi.edu)
Network Manager, WPI

April 19th, 2001

To Whom It May Concern:

We sent the following letter to you Saturday, April 14th. We are writing again to ascertain whether your school would be willing to participate. [College]'s participation would be very valuable to our project, and any assistance you could offer would be greatly appreciated.

We thank you in advance for your time.

Sincerely,
Adam Joseph Augusta (roxton@wpi.edu)
Michael Allan Narris (mnarris@wpi.edu)

Project Advisors:
Mark Claypool, Assistant Professor (claypool@wpi.edu)
Robert Kinicki, Associate Professor (rek@wpi.edu)

July 26th, 2001

Two Whom It May Concern:

As part of our Interactive Qualifying Project at Worcester Polytechnic Institute of Worcester, Massachusetts, we are conducting a 5-7 minute survey to collect information on effects and perceptions of network use policy on students. Your college was one of eight selected in a case study of United States colleges with similar characteristics.

We request permission to deploy the following e-mail survey to a portion of [College]'s undergraduate students at the beginning of the fall semester. If you and your school would be willing to participate in this survey, we would require at least 100 randomly selected undergraduate student e-mail addresses.

Please send an address list or an e-mail alias to usepolicy@wpi.edu. The contact information and the data collected will be held strictly anonymous and will be used for academic purposes only.

If you have any concerns, you may opt to personally distribute the survey electronically within the school. If you choose to do so, please notify us prior to its release.

For more information regarding our project, please visit the following URL: http://www.wpi.edu/~roxton/IQP/ProjectInfo.html

We encourage you to participate in the survey as well.

Thank you for your time.

Sincerely,
Adam Joseph Augusta (roxton@wpi.edu)
Michael Allan Narris (mnarris@wpi.edu)

Project Advisors:
Mark Claypool, Assistant Professor (claypool@wpi.edu)
Robert Kinicki, Associate Professor (rek@wpi.edu)

Special Thanks to:
James Doyle, Associate Professor (doyle@wpi.edu)
Allan E. Johannesen (aej@wpi.edu)
Director of Internetworking, WPI
Sean M. O'Connor (soconnor@wpi.edu)
Network Manager, WPI

August 11th, 2001

To Whom It May Concern:

We sent the following letter to your facilities Thursday, July 26th. We would be very interested in distributing our survey to [College]'s student body at the beginning of the fall semester.

Other universities have already opted to participate in our study, and [College]'s participation would be highly valuable in our efforts. We request that you either affirm or decline participation so that we may research another reasonable test case in your geographic region.

If you feel we have sent this to you in error, we would ask that you please send us the contact information of a faculty member of appropriate capacity. If you would like to discuss the matter verbally, please leave us your office number and a timeframe within which we should call. Adam can be reached at (508) 752-8495.

We thank you in advance for your time.

Sincerely,
Adam Joseph Augusta (roxton@wpi.edu)
Michael Allan Narris (mnarris@wpi.edu)

Project Advisors:
Mark Claypool, Assistant Professor (claypool@wpi.edu)
Robert Kinicki, Associate Professor (rek@wpi.edu)

September 6th, 2001

To Whom It May Concern:

I am writing with respect to the WPI Project Survey we wish to distribute to the undergraduate students of [College]. Our project advisors have requested that we set a firm date at which time we will formally tally all abstaining contacts as declinations. This date is next Monday, September 10th. We hope to distribute our survey during the coming week and would like to know if your school is interested in participating. Your school's participation would be invaluable to our efforts. We would appreciate it if you would please send us a final answer with respect to our inquiry as soon as reasonably possible.

Thank you very much for your time.

Sincerely,
Adam J. Augusta
Michael A. Narris

September 13th, 2001

To Whom It May Concern:

My partner and I understand that many of the systems are not designed for the straightforward extraction of e-mail addresses, especially in a random fashion with criteria such as class. With this in mind, my partner and I have independently generated a list of valid undergraduate e-mail addresses.

We will not, of course, use this list without the permission of [College]'s technical staff. I ask that you please indicate whether you will allow or disallow the distribution of our survey.

For the latest updates on our project, please visit:
http://www.wpi.edu/~roxton/IQP/ProjectInfo.html

If you have any questions or concerns, please do not hesitate to contact us.

Sincerely,
Adam J. Augusta
Michael Allan Narris

Appendix D: College Web Page URLs and Addresses

Worcester Polytechnic Institute
100 Institute Road
Worcester, MA 01609
http://www.wpi.edu

Clark University
950 Main St
Worcester, MA 01610
http://www.clarku.edu

Illinois Institute of Technology
3300 South Federal Street
Chicago, IL 60616
http://www.iit.edu

The University of Chicago
5801 South Ellis Ave.
Chicago, IL 60637

Harvey Mudd College
301 E. 12th Street
Claremont, CA 91711
http://www.hmc.edu

Pitzer College
1050 N. Mills Ave.
Claremont, CA 91711
http://www.pitzer.edu

Georgia Institute of Technology
Atlanta, GA 30332
http://www.gatech.edu

Emory University
Atlanta, GA 30322
http://www.emory.edu

Appendix E: Acceptable Network Use Policies

Worcester Polytechnic Institute Acceptable Network Use Policy:
Summary of the Rules

Comply with Intended Use of the System

Don't violate the intended use of the systems and network at WPI.

Assure Ethical Use of the System

Don't let anyone know your password(s).

Don't violate the privacy of other users.

Don't copy or misuse copyrighted or licensed material.

Don't use the systems or network to harass anyone in any way.

Assure Proper Use of System Resources

Don't abuse your e-mail, Web, or other communications privileges.

Don't perform commercial activities on WPI facilities.

Don't interfere with the functioning of the network or computer systems.

Massachusetts Computer Crime Law

Comply with Intended Use of the System

It is important that you understand the purpose of the systems and network so that your use of these resources is in compliance with that purpose.

Don't violate the intended use of the systems and network at WPI.

The purpose of these facilities is to support research, education, and WPI administrative activities, by providing access to computing resources and the opportunity for collaborative work. All use of the WPI network must be consistent with this purpose. For example:

- Don't try to interfere with or alter the integrity of the system at large, by doing any of the following:
  - permitting another individual to use your account.
  - impersonating other individuals in communication (particularly via forged email, talk, news, etc.).
  - attempting to capture or crack passwords or encrypted information.
  - destroying or altering data or programs belonging to other users.
- Don't try to restrict or deny access to the system by legitimate users. e.g.
  - don't try to crash systems or networks, either at WPI or off campus.
  - don't attempt to make a computer impersonate other systems.
  - don't consume unneeded resources; to include network bandwidth, compute time, disk, or processes. The web has traffic limitations; a site without an academic mission should not consume extensive resources.
- Don't use the facilities for private financial gain.
- Don't transmit threatening or harassing materials.

Assure Ethical Use of the System

Along with the many opportunities that the computer systems and networks provide for members of the WPI community to share information comes the responsibility to use the system in accordance with WPI standards of honesty and personal conduct. Those standards, outlined elsewhere in this manual, call for all members of the community to act in a responsible, professional way.

Appropriate use of the resources includes maintaining the security of the system, protecting privacy, and conforming to applicable laws, particularly copyright and harassment laws.

2. **Don't let anyone know your password(s).**
   While you should feel free to let others know your username (this is the name by which you are known to the whole Internet user community), you should **never** ever let anyone know your account passwords. This includes even trusted friends, and computer system administrators (e.g. the College Computer Center staff). You will note that you specify a one-time password and your choice of login name to the operator to gain CCC UNIX system access. When you first use that password to login you must specify a personal password. This assures you that you are not sharing

knowledge of your password with a staff member. We have taken this step so that your password is private to you; please maintain that secrecy.

Giving someone else your password is like giving them a signed blank check, or your charge card. You should never do this, even to "lend" your account to them temporarily. Anyone who has your password can use your account, and whatever they do that affects the system will be traced back to your username -- if your username or account is used in an abusive or otherwise inappropriate manner, you can be held responsible. Much of the software on the WPI computer systems are licensed only for current students, staff, and faculty; use of the computers by others violates that contract.

In fact, there is never any reason to tell anyone your password: every WPI student, faculty member, or on-campus staff person who wants an account of his or her own can have one. If your goal is permitting other users to read or write some of your files, there are always ways of doing this without giving away your password.

For information about how to manage the security of your account, including advice on how to choose a good password, how to change passwords, and how to share information without giving away your password, see the on-line documentation or email to helpdesk.

3. **Don't violate the privacy of other users.**
   The Electronic Communications Privacy Act (18 USC 2510 et seq., as amended) and other federal laws protect the privacy of users of wire and electronic communications.

   The computer and network facilities of WPI facilitate information sharing. Security mechanisms for protecting information from unintended access, from within the system or from the outside, are minimal. These mechanisms, by themselves, are not sufficient for a large community in which protection of individual privacy is as important as sharing. Therefore, you must supplement the system's security mechanisms by using the system in a manner that preserves the privacy of themselves and others.

   All users should make sure that their actions don't violate the privacy of other users, if even unintentionally.

   Some specific areas to watch for include the following:

- Don't try to access the files or directories of another user without clear authorization from that user. Typically, this authorization is signaled by the other user's setting file access permissions to allow public or group reading of the files. If you are in doubt, ask the user.
- Don't try to intercept or otherwise monitor any network communications not explicitly intended for you. These include logins, e-mail, user-to- user dialog, and any other network traffic not explicitly intended for you.
- Unless you understand how to protect private information on a computer system, don't use the system to store personal information about individuals which they would not normally disseminate freely about themselves.
- Don't create any shared programs that secretly collect information about their users. Software on on the WPI computer systems and network is subject to the same guidelines for protecting privacy as any other information-gathering project at the Institute. This means, for example, that you may not collect information about individual users without their consent.
- Don't remotely log into (or otherwise use) any workstation or computer not designated explicitly for public logins over the network -- even if the configuration of the computer permits remote access -- unless you have explicit permission from the owner and the current user of that computer to log into that machine.

Don't copy or misuse copyrighted or licensed material.

Copyright

Copyright is a form of protection provided by the laws of the United States (title 17, U.S. Code) to the authors of *original works of authorship* including literary, dramatic, musical, artistic, and certain other intellectual works. This protection is available to both published and unpublished works.

You should assume materials you find on the Internet are copyrighted unless a disclaimer or waiver is expressly stated. Note that there does not have to be a statement that the material is copyrighted for it to be copyrighted; any original work created in recent years is automatically copyrighted according to U.S. law. The copyright holder has extensive rights. You must contact the copyright holder and ask permission to display the material.

If you do not abide by these legal and contractual restrictions, you may be subject to civil or criminal prosecution.

Although this is not an exhaustive list, you are likely to violate copyright by:

- displaying pictures or graphics you have not created.
- offering sound recordings you have not recorded yourself. Even if you have recorded them, you must have permission from the copyright holder.
- placing any materials owned by others, i.e. copyrighted works, on your Web page, or for other display, without the expressed permission of the copyright owner. (Examples: cartoons, articles, photographs, songs, sound bites, software, graphics scanned in from published works or other web pages).

  Placing copyright attribution on the displayed material is not sufficient to enable its display; you must contact that copyright owner to be assured that the display is acceptable. Do this *before* display is attempted.

Fair Use

Educational institutions enjoy special exemptions from copyright protection, called *Fair Use*, whereby reasonable portions of copyrighted material may be distributed by instructors to students in a class. If copyrighted materials are to be placed on the web for a course, the materials must be restricted to the course. We offer assistance to accomplish this end. All class materials do not have to be protected in this way, but if the instructor places the information which is copyright protected in its own directory in the web and then uses a web page we designed to restrict logins to a class it will be acceptably protected. The fair use code is simple, but for further information, please see the Stanford University Copyright and Fair Use World Wide Web site.

Licenses

The programs offered for use on the campus computers typically have licenses which restrict use to the computer where they are installed and for educational purposes. The software is usually copyrighted, too. Although this is not an exhaustive list, you are likely to violate license and/or copyright by:

- reselling or giving away licensed programs or data

- using educational-licensed programs or data for non-educational purposes
- using programs or data for financial gain
- using programs or data without being among the individuals or groups licensed to do so

Don't use the systems or network to harass anyone in any way. Harassment is defined as any conduct, verbal or physical, on or off campus, which has the intent or effect of unreasonably interfering with an individual's or group's educational or work performance at WPI or which creates an intimidating, hostile or offensive educational, work or living environment. Harassment on the basis of race, color, gender, disability, religion, national origin, sexual orientation, or age includes harassment of an individual in terms of a stereotyped group characteristic, or because of that person's identification with a particular group.

The Institute's harassment policy extends to the networked world. For example, sending email or other electronic messages which unreasonably interfere with anyone's education or work at WPI or any other institution, using WPI as a base, may constitute harassment and is in violation of the intended use of the system. Do not print or display material that may be considered offensive unless you have an academic reason. This includes pornography, both pictures and written material.

Any member of the WPI community who feels harassed is encouraged to seek assistance and resolution of the complaint. To report incidents of on-line harassment, send email to the helpdesk. If you believe you are in danger, call the Campus Police immediately at x5433.

Assuring Proper Use of the System

WPI's computer and network resources are powerful tools that can be easily misused. Your use of the system should be consistent with the intended uses of these resources. In particular, you should not overload the systems or otherwise abuse the network.

Assure Proper Use of System Resources

WPI's computer and network resources are powerful tools that can be easily misused. Your use of the system should be consistent

with the intended uses of these resources. In particular, you should not overload the systems or otherwise abuse the network.

Don't abuse your electronic mail (email), web, or other communications privileges.
Electronic mail is a fast, convenient form of communication. It is easy to send electronic mail to multiple recipients, and you can even send a message to many recipients simply by specifying a single list name (i.e., by using a mailing list). However, this ability to send messages to many people makes it easy to misuse the system. The general rule is: use email to communicate with other specific users, not to broadcast announcements to the user community at large.

For example, while it is appropriate to use email to have an interactive discussion with a set of people (even 20 or more users) or to use email to send a single copy of an announcement to some "bulletin board" facility with a wide readership (e.g. Network News, or an event), it is not appropriate to use email as a way to broadcast information directly to a very large number of people (e.g., an entire WPI class). This is true whether you include the recipient usernames individually or by using a mailing list: under no circumstance should you use the email system to get a general announcement out to some large subset of the WPI community.

These guidelines are not based on etiquette alone: the mail system simply does not have the capacity to process a very large number of email messages at once. When a user sends out an announcement to a huge list of recipients, the mail servers get overloaded, disks fill up, and staff intervention is required. The overall result is a negative impact on the quality of service provided for all users.

Finally, the proliferation of electronic chain letters is especially abusive of the mail system and the network. Chain letters waste valuable computing resources, and may be considered harassing. Creating or forwarding chain letters may subject you to Institute disciplinary proceedings.

The web has specific traffic limitations; a site without an academic mission should not consume extensive resources.

The web at WPI has a multitude of uses. Potential students can learn about WPI and even apply to WPI. Researchers can get information on programs at WPI. Alumni can peruse information especially for them. Students, faculty, and staff can offer their web pages. Unfortunately, excessively popular pages can swamp the web so that these functions cannot be accomplished.

Any individual whose site gets 3% of the usage of the entire WPI web will be warned to reduce the traffic on their web. They will have 1 week to bring the traffic down to a reasonable level. 3% may not sound like much, but that is actually a large fraction of the resource, given how many people at WPI are sharing the resource. A site will be shut down if the owner has not managed to tame their web within a week.

A site which is over 5% of the traffic will be shut down immediately, as an emergency measure to preserve web functionality. Other grounds for immediate shutdown are copyright violations, commercial ventures, and other Acceptable Use Policy violations.

It is possible that some web page, which is consistent with the academic mission of WPI, will become very popular, and we will try to deal with that situation should it arise. We have not yet seen crippling traffic problems from any pages of this sort, however.

Don't perform commercial activities on wpi facilities.

- Commercial activity on the WPI network is only permitted for business done on behalf of WPI or its organizations, not for the benefit of private individuals or other organizations without authorization.
- It is not permitted to run a private business on the WPI network.
- The Institute's name must not be used in ways that suggest or imply the endorsement of other organizations, their products, or services.
- Fundraising and advertising may be conducted on the WPI network only under the supervision of officially recognized campus organizations.
- Reselling network IP services over WPI's network is not permitted.

Don't interfere with the functioning of the network or computer systems.
Your computer and network devices must not perform actions that might interfere with others at WPI. e.g.

- Broadcast a storm of packets, causing excessive network traffic, making the network run slowly for others.
- Run wireless networking equipment not authorized by WPI Network Operations, with the inherent possibility of interference with WPI's wireless networks.
- Run processes on computers which bog them down, making them less useful for others in the WPI community

The Massachusetts Computer Crime Law

The Massachusetts Computer Crime Law, enacted on January 24, 1995 has four points:

Any unauthorized access into any computer system, either directly, by network, or by telephone is prohibited.

All electronically stored or processed data is now deemed as "property". As such, any destruction or corruption of such data is illegal.

Electronic copies of files will now be admissible as evidence in court.

Computer crime can now be prosecuted and punished in either the county where the perpetrator was physically located or in the county of the computer system and data that were accessed.

Clark University Acceptable Network Use Policy:

Computer Resource Policy

Policy on Appropriate Use of Clark's Computing Resources

I. Introduction

Clark University values the free expression of ideas, and provides and maintains computer and network resources to support the education, research and work of students, faculty, and staff at Clark. "Clark's computing resources" include computers, networks and network connections, software, and licenses. This policy applies to all users of Clark's computing resources. The use of Clark's computing resources is subject to the terms and conditions outlined below. It is every user's responsibility to understand and comply with these regulations.

II. Acceptable Use

General use of Clark's computing resources is deemed to be acceptable except as defined below.

A. Illegal/Prohibited Uses

Clark's computing resources may not be used for purposes which may be considered civil or criminal offenses or which violate Clark's official standards governing behavior in general. Examples of such official standards include those in the Student Handbook, the Faculty Handbook, the Sexual Harassment Policy, and the Administrative and Staff Handbooks. Examples of illegal or prohibited behavior include, but are not limited to:

Destroying or damaging equipment, software, or data,
Posting or transmitting harassing, obscene, or threatening material,
Posting or transmitting libelous or slanderous material,
Violating software or network license agreements,
Disrupting or monitoring communications without authorization,
Violating copyright laws, and
Violating the privacy of other users.

B. Commercial Use

Clark's computing resources may not be used for commercial purposes on behalf of individuals, businesses, or institutions other than Clark. Use of Clark's resources for commercial purposes on behalf of Clark is subject to administrative approval.

C. Resource Utilization

Clark's computing resources are provided primarily to support the education, research, and work of members of the Clark community. Use of these resources for other purposes may be restricted if they interfere with primary uses.

D. Miscellaneous

Certain activities specific to Clark's computing resources are also prohibited

by this policy. Specifically, users may not: Violate or attempt to violate the security of any system,
Send messages, such as e-mail, faxes, or voice mail, under the name of another user, or
Use computer accounts or network identification numbers assigned to others without official permission.

III. Communication and Editorial Control
A. Communication
Clark University recognizes the importance of communication in its mission of education and research. Clark supports the use of its computing resources for communication, and provides and supports several communication media, for example, e-mail, web pages, and the Bulletin system.
B. Editorial Control
Communications based on or transmitted by Clark's computing resources are divided into two categories. The first category comprises communications that are official statements of the University. Examples of such communications include the University's official web pages, departmental web pages, and messages posted in University moderated bulletin folders.
The second category comprises all other communications. Examples of communications in this category include the personal web pages of faculty, staff, alumni, and students, web pages of student organizations, e-mail, and messages posted in public forums not moderated by the university.
The University assumes complete editorial control over communications in the first category, but is not responsible for communications in the second category. Individuals who use Clark's computing resources for communications are responsible for ensuring that this use does not violate any provision of the Acceptable Use section of this policy.
IV. System Administration
Clark's computing resources are administered by a variety of departments and individuals. Clark's central computer system and network are administered by the Office of Information Systems. In addition, there are computers and sub networks that are administered within departments. All individuals with administrative responsibility are required to observe the following standards.
A. Maintenance of Editorial Divisions
Administrators of systems used for communication (see Sec. III) should ensure that documents containing official statements of the University have appropriate content and are appropriately identified as such, with appropriate disclaimers, in situations where there might be confusion.
B. System Administrators' Respect for Privacy
System administrators will respect the privacy of the users of systems under their control. They will not examine, nor allow others to examine (except as noted in Sec. V.B.) the files or e-mail of users without permission except in situations where it is necessary for system administrators to ensure or restore the proper functioning of the system. In the event that it is not possible to obtain permission, the user and the Information Technology Advisory Committee

will be notified promptly.

V. Procedures

A. Distribution of Policy Statements

This policy will be made available to every user of Clark's computing resources and maintained as an official communication of the University. It will be given to each new user and posted in computer labs.

B. Initial Complaint Procedure

The University has designated several persons to respond to complaints about violations of this policy. If the alleged offender is:

- A student, complaints may be sent by e-mail to dsoffice@clarku.edu or in writing to the Dean of Students,
- A faculty member, complaints may be sent by e-mail to provost@clarku.edu or in writing to the Provost, or
- A member of the staff, administration, or any other user not specified previously, complaints may be sent by e-mail to mailto:humanresources@clarku.edu or in writing to the Director of Human Resources.

The University will respect the privacy of users of its systems and not allow frivolous inspection of users' e-mail or other files. However, access may be necessary in situations that call for the investigation of a complaint, determined by one of the university administrators above to be reasonable, or when compelled to do so by law. In such situations the user and the Information Technology Advisory Committee will be notified promptly.

Upon receiving a complaint that is found to be substantive, the alleged offender will be notified that he/she or someone using their account has been the subject of a complaint. This notification will explain the alleged violation and instruct the alleged offender to take steps to ensure that there are no future violations, for example, by securing his/her account or by ceasing his/her actions. The notification need not identify the complainant.

C. Referral to Appropriate Board/Committee

In the case of a particularly serious violation, repeated violations, or if the alleged offender contests the violation, cases will be referred to regular disciplinary channels and all relevant information or evidence will be made available to the disciplinary authority.

Illinois Institute of Technology's Acceptable Network Use Policy:

Computing and Network Services Policies
Computer Use Policy

Policies for Computer Use - from the IIT Student Handbook
The IIT computer network consists of a campus-wide network, local area networks, and time-shared computers, as well as personal computers. Computing and Network Services provides access to the network for IIT students, faculty, and staff in support of the educational mission of the university. IIT does not monitor or review material prior to transmission on university-owned networks.

Rights
Members of the IIT community can expect certain rights as they use the network and its services.

Privacy:
All members of the community have the right to privacy in their electronic mail. However, electronic communications are by no means secure, and users must recognize that during the course of ordinary management of computing and network services, network administrators may view user files. In addition, if a user is suspected of violations of the responsibilities stated in this policy, or of violating other university policies, or of criminal activity, that user's right to privacy may be superseded by IIT's desire to protect members of the IIT community and its commitment to maintain the network's integrity and the rights of all network users. Should the security of a system be threatened, user files may be examined under the direction of the CNS staff, or other authorized personnel.

Safety:
While unwanted or unsolicited contact cannot be controlled on the network, network users who receive threatening communications should bring them to the attention of CNS, the appropriate network administrator, or the Office of Student Affairs. Users must be aware, however, that there are many services on the Internet that might be considered offensive to groups of users, and therefore, network users must take the responsibility for their own navigation of the network.

Standards
Opinions expressed on the network may not be represented as

the views of IIT. Student users of the network are subject to the IIT Code of Conduct set forth in the student handbook, as well as the policies on sexual harassment, unlawful discrimination, academic honesty, and other applicable policies. IIT faculty and staff users are subject to all IIT policies, including those prohibiting unlawful discrimination and harassment, and other disciplinary procedures as set forth in the IIT Procedures Manual. All users are subject to applicable state and federal laws.

Responsibilities

There are also responsibilities that must be met as part of the privilege of network access. Network users are expected to live up to these responsibilities. A user who knowingly violates a network responsibility may have his/her network access suspended. It is the responsibility of the user to inquire about the appropriateness of an action or use prior to execution.

A network user is responsible for the use of his/her account, and a) may not give anyone else access to that account, b) may not use an IIT computer account that was not assigned to him/her, c) may not try in any way to obtain the password for another user' s computer account, and d) may not attempt to disguise the identity of the account or machine he/she is using or represent him/herself to be another user.

Network users are responsible for the security of their passwords. This includes changing one's password on a regular basis and making sure no one else knows it.

Network users must not use IIT's network resources to gain or attempt to gain unauthorized access to remote computers.

Network users must not deliberately perform an act which will disrupt the normal operation of computers, terminals, peripherals, or networks. This includes, but is not limited to, tampering with components of a local area network (LAN) or the high-speed backbone network, otherwise blocking communication lines, or interfering with the operational readiness of a computer.

Network users must not run or install on any of IIT's computer systems, or give to another, a program which is intended to or likely to result in the eventual damage of a file or computer system and/or reproduction of itself. This includes, but is not limited to, the classes of programs known as computer viruses, bots, Trojan horses, and worms.

Network users must not attempt to circumvent data protection schemes or exploit security loop holes.

Network users must abide by the terms of all software licensing agreements and copyright laws, and may not make copies of or make available on the network copyrighted material, unless permitted by a license.
Network users must not perform acts which are deliberately wasteful of computing resources or which unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, creating unnecessary multiple jobs or processes, obtaining un-necessary output, or printing or creating unnecessary network traffic. Printing excessive copies of any documents including resumes, theses, and dissertations is also prohibited.
Network users must not attempt to monitor another user's data communications, nor read, copy, change, or delete another user's files or software without permission of the user.
CNS resources are provided to support the educational mission of IIT. These resources may not be used for commercial purposes.

CNS, and other appropriate IIT authorities should be notified about violations of computer laws and policies, as well as about potential loopholes in the security of its computer systems and networks.
When violations are reported, network administrators may suspend network privileges pending investigation. Account holders will be notified as soon as reasonably possible. Upon investigation of the alleged violation, the network administrator may reinstate network privileges or, if the violation involves an IIT student, may refer the matter to the Office of Student Affairs. The Office of Student affairs may investigate the alleged violation and determine the sanction, or may refer the matter to the Campus Judicial Board for adjudication. If the alleged violation is committed by a member of the staff or faculty, then the offense will be treated as misconduct under the appropriate section of the IIT Procedures Manual or Faculty Handbook.
Violators of this policy may be denied access to the IIT computer network, in addition to other applicable disciplinary procedures.

Updated by Webgroup

CNS Policies

Overview
IIT Computer Use Policy
IIT World Wide Web Policy
Client Services Policies
Galvin Library: Policy for Computing Resources
Abuse Response Policy for Unauthorized Use of CNS

Updated on Wednesday, September 20, 2000 by Webgroup
© 2001 IIT Webgroup

University of Chicago's Acceptable Network Use Policy:

Eligibility & Acceptable UseThe University of Chicago
Eligibility and Acceptable Use Policy for Information Technology

See also: NSIT Accounts Eligibility supplemental document
The University of Chicago provides information technology for educational, research, and administrative applications by its students, faculty, and staff. This Eligibility and Acceptable Use Policy stems from the University's Statutes and Bylaws and from its more general policies and procedures governing faculty, students, staff, and facilities.1 With only a few exceptions, the present policy simply applies these larger policies and procedures to the narrower information-technology context. It balances the individual's ability to benefit fully from information technology and the University's need for a secure and reasonably allocated information-technology environment.
In general, University faculty, students, and staff may use University information technology (which includes privately-owned computers connected to the University network) in connection with the University's core teaching, research, and service missions. Certain non-core uses that do not consume resources or interfere with other users also are acceptable. Under no circumstances may faculty, students, staff, or others use University information technology in ways that are illegal, that threaten the University's tax-exempt or other status, or that interfere with reasonable use by other members of the University community. Violations of information-technology rules and policies typically result in University disciplinary action, which may have serious consequences.
The information-technology Eligibility and Acceptable Use Policy begins with a few principles, defines several categories into which users and applications of information technology fall, and specifies which users may use University information technology for which applications. The footnotes in this document provide explanations, illustrations, and examples of how the policy works in practice, but it is the policy, and not the explanatory material, which governs specific instances.

Principles
Three general principles underlie eligibility and acceptable-use policies for information technology:

- University information technology is for University faculty, students, and staff to use for core University purposes.
- Any use counter to this, or which interferes with core use by others, is unacceptable.
- Some applications of University information technology are unacceptable even if they serve core purposes.

Definitions
University Information Technology

Any computer, networking device, telephone, copier, printer, fax machine, or other information technology which

- is owned by the University or
- is licensed or leased by the University

is subject to University policies. In addition, any information technology which

- connects directly to the University data or telephone networks,
- uses University network-dialup facilities (the campus modem pool),
- connects directly to a computer or other device owned or operated by the University, and/or
- otherwise uses or affects University information-technology facilities

is subject to University information-technology policies, no matter who owns it.2

Users

Three broad classes of potential users have different privileges:

- Regular Users, who are entitled to use all or most University technology and services,
- Special Users, who are entitled to use specific limited services for specific purposes under specific conditions, and
- Excluded Users, who are not entitled to use University information technology.

Regular Users

In general, only current undergraduate and graduate students3 and current non-temporary regular faculty and staff4 of the University are Regular Users. Faculty, student, and staff status does not extend to family members or colleagues who are not themselves Regular Users.

Special Users

Special Users comprise certain individuals and specified classes of University affiliates to whom the University provides a tightly limited subset of University information technologies and services. The specified special-user classes consist primarily of certain organizations affiliated with the University and their staff and of certain categories of students. They also include certain individuals working temporarily at the University under the explicit sponsorship of an administrative or academic department.5 The Chief Information Officer authorizes special-user classes and individual special users, under the authority of the President. The Chief Information Officer determines which individuals or organizations on campus are responsible for use (or misuse) of information technology by Special Users and any associated costs. Special Users abide by all relevant University policies. In general, they reimburse the University or pay directly for the cost of the services they receive. Special User privileges may end without notice. Special Users in a specified class retain no University information-technology privileges once they leave that class. Individual Special Users receive privileges only for a period specified at the outset.

Excluded Users

These are all individuals or organizations that are not Regular Users or Special Users.

Applications

Here again three distinct categories are important:

Core applications, those clearly associated with the University's core education, research, or service, either directly or through University administration,

Restricted applications, those clearly unrelated to the University's core purposes, or which violate general University policies, jeopardize its tax-exempt or other circumstances, or otherwise interfere with core applications, and

Ancillary applications, which do not fall clearly into either of the preceding two categories and which do not interfere with Core applications.

Core Applications

These support University instruction, research, service, and administration. Classroom use, computer-based assignments, research applications, communication among faculty, students, and administrators, administrative applications, access to University-related information, and similar applications all are Core applications.

Restricted Applications

Restricted applications of University information technology primarily include

those that threaten the University's tax-exempt status, such as certain kinds of political activity and most commercial activity,

those that are illegal, such as fraud, harassment, copyright violation, and child pornography,

those that deprive other users of their fair share of University information technology or interfere with the functioning of central networks and systems, such as mass mailings, chain letters, unauthorized high-bandwidth applications, or denial-of-service attacks, and

those that violate more general University Statutes, Bylaws, and policies.

Disclaimers do not render Restricted applications acceptable. The only recourse available to someone interested in such applications is to use non-University computers, networks, and other technologies.

Ancillary Applications

Ancillary applications are easy to list, but difficult to define. Examples are plentiful: using a University phone to make a dentist appointment, a University-connected personal computer to host small-scale personal (but non-commercial) Web pages, University servers to send and receive for modest amounts of personal electronic mail, a University fax machine to get a vacation itinerary from a travel agent, and the like. In general, Ancillary applications are those neither explicitly permitted nor explicitly restricted, and with one other essential attribute: they are invisible to other users, to network and system administrators, and to other University offices. Ancillary applications consume only resources that would otherwise go to waste, and never require any action or intervention by anyone at the University other than their user. As a rule, Ancillary applications that become visible to others or burden systems are ipso facto no longer Ancillary, but Restricted.

Eligibility and Acceptable Use

No one may use University information technology for Restricted purposes without explicit written authorization from the Chief Information Officer, who consults the President, the Provost, the General Counsel, and other officials as appropriate.

Except for the preceding restriction, Regular Users may use the full array of University information technology for Core applications. Only Regular Users are eligible to use most centrally-funded technology, including public computing clusters and classrooms, and University help desks and technical support. Except for a few specific exceptions, only Regular Users are eligible to use the University data network, including its dialup modem pool.6

There is one major exception to Regular Users' general rights to use information technology for Core applications. If any application of information technology, however permissible otherwise, disables computers or network services, consumes disproportionate enough resources that other users are denied reasonable access to information technology, or induces substantial costs outside the user's Department, then that application is Restricted.7

In general, Regular Users also may use campus telephones, the campus network, and personally or departmentally owned computers for Ancillary applications.8 However, even Regular Users may not use information technology in ways that interfere with others,9 or that consume University resources other than those directly under the user's control.10 In general, any Ancillary use of the University network that becomes apparent to other users thereby becomes Restricted, and unacceptable.

Special Users may use University information technology only insofar as they are specifically authorized to do so.

Except for certain materials and facilities the University explicitly makes available to the general public, Excluded Users may not use University information technology in any way.

Where definitions of user or application status are unclear, or where patterns of use appear to be out of compliance with this policy, the Chief Information Officer provides interpretations or direction as appropriate on behalf of the President and the University. Where necessary, the Chief Information Officer consults the President, other Officers of the University, General Counsel, and the Board of Computing Activities and Services for further advice and guidance.

Roles and Responsibilities

The University

The University owns most of the computers and all of the internal computer networks used on campus. The University also has various rights to the software and information residing on, developed on, or licensed for these computers and networks. The University (including central organizations and academic Divisions, Schools, and Departments) administers, protects, and monitors this aggregation of computers, software, and networks. In its management of information technology, the University and its administrative and academic departments take responsibility for

- Focusing central information technology resources on activities connected with

instruction, research, and administration;
Protecting University networks and other shared facilities from malicious or unauthorized use;
Ensuring that central University computer systems do not lose important information because of hardware, software, or administrative failures or breakdowns;11
Managing computing resources so that members of the University community are not denied fair access to them;12
Establishing and supporting reasonable standards of security for electronic information that community members produce, use, or distribute, and ensuring the privacy and accuracy of administrative information that the University maintains;
Delineating the limits of privacy that can be expected in the use of networked computer resources and preserving freedom of expression over this medium without countenancing abusive or unlawful activities;
Monitoring policies and communicate changes in policy as events or technology warrant; and
Enforcing policies by restricting access and initiating disciplinary proceedings as appropriate.13

The Individual

The University of Chicago supports networked information resources to further its mission of research and instruction and to foster a community of shared inquiry. All members of the University community must be cognizant of the rules and conventions that make these resources secure and efficient. Users of University information technology take responsibility for

Using resources efficiently, and accepting limitations or restrictions on computing resources - such as storage space, time limits, or amount of resources consumed - when asked to do so by systems administrators;
Protecting passwords and and respecting security restrictions on all systems;14
Backing up files and other data regularly;15
Preventing unauthorized network access to or from their computers or computer accounts;16
Recognizing the limitations to privacy afforded by electronic services;17
Respecting the rights of others to be free from harassment or intimidation, to the same extent that this right is recognized otherwise on campus; and
Honoring copyright and other intellectual-property rights.

Sanctions and Procedures

When any use of information technology at the University presents an imminent threat to other users or to the University's technology infrastructure, system operators may take whatever steps are necessary to isolate the threat, without notice if circumstances so require. This may include changing passwords, locking files, disabling computers, or disconnecting specific devices or entire sub-networks from University, regional, or national voice and data networks. System operators restore connectivity and functionality as soon as possible

after they identify and neutralize the threat.
Telephones, computers, network connections, accounts, usernames, authorization codes, and passwords are issued to Regular Users and Special Users to identify them as eligible users of University information technology. Users are responsible for not sharing their privileges with others, and especially for ensuring that authorization codes and passwords remain confidential. Users of computers connected to the campus network, permanently or temporarily, are responsible for ensuring that unauthorized users do not thereby gain access to the campus network or to licensed resources.
Use of information technology that violates this Policy and rules based on it may result in disciplinary proceedings and, in some cases, in legal action. Disciplinary proceedings involving information technology are the same as those for violations of other University policies, and may have serious consequences. Unauthorized use of University information technology by Excluded Users may result in police intervention or legal action.
April 2000

1 The present document updates and extends the "Provost's Policy on Information Technology Resources" last revised in 1995. Since 1995 the interconnection, pervasiveness, and importance of information technology at the University have grown. The susceptibility of individual devices to network-based interference from others and the infiltration of non-University users into the campus network, neither anticipated by the earlier policy, have increased dramatically. Moreover, the earlier document did not address eligibility. The Eligibility and Acceptable Use Policy for Information Technology is implemented by the Chief Information Officer under the authority of the President, in consultation with the Board of Computing Activities and Services.

2 A computer owned personally by a student, faculty member, or staff member is subject to University policy while it connects to the University network directly or through a dialup connection. An individual may not grant access privileges to other individuals on a computer in violation of the general eligibility policy below, even if that computer is personally owned. If a computer is connected to the University network, access from that computer to the rest of the campus network can only be made available to individuals otherwise authorized to use the campus network. This includes email, Web services, file transfer, Internet Relay Chat (IRC), telnet, and any other network traffic. The only major exceptions to this are three. So long as it does not interfere with use of the network by others, a computer on the University network in general may function as a Web server to outsiders. It may allow file transfer to and from itself (but not other computers). It may host mailing lists including non-University individuals. Conversely, a computer on the University network in general may not provide proxy Web service to outsiders. It may not provide email services to outsiders (or otherwise enable outsiders to identify themselves as being at the University of Chicago). It may not permit outsiders to use telnet or similar protocols

to reach other computers on campus or elsewhere.
3 The Registrar determines who is a current student, following categories and policies outlined in the Student Information Manual, and provides this information directly to Networking Services and Information Technologies (NSIT) and other organizations.
4 University Human Resources Management determines who is a member of the faculty or staff. In certain specific cases NSIT and academic or administrative Departments agree on authorization and database mechanisms to deal with special cases such as visiting faculty, temporary staff, and long-term consultants. In general, however, eligibility for the full array of information-technology services is determined by permanent-staff status in central University databases.
5 For example, some affiliated organizations purchase telephone services from NSIT Voice & Data Networking (such as the University Hospitals) or buy computers through its Campus Computer Stores (such as the Lutheran Theological Seminary and NORC). Members of these organizations and certain other individuals (for example, faculty, student, and staff family members, and University alumni) may use the University's fee-for-service dialup modem pool at the University's negotiated rates. Individuals with appropriate Library privileges may use online databases and other materials accessible therein.
6 The "free" campus modem pool is only for Core applications. Regular Users who need dialup access for other purposes, such as family access to the Internet or private consulting, must use the University's fee-for-service dialup provider or another Internet service provider at their own expense.
7 Just because a given application does not violate information-technology policy the application itself is not otherwise defensible. For example, a student who posts on a public Web site the answers to a test other students have yet to take may not be violating information-technology policies, but he or she almost certainly is violating the University's rules against cheating.
8 A classic example of acceptable Ancillary use is a staff member using a University phone to order a birthday cake for a son or daughter. (Whether this interferes with work is a larger, non-technological issue.) Much private email sent over the University network is precisely analogous: the individual who sends and receives it gains convenience, a tangible benefit, while the University and other members of its community lose nothing. Even if some applications such as these cause small costs - such as local-call costs, or small amounts of printing - they remain acceptable in much the way similar non-technological costs have always been.
9 A classic example of apparently Ancillary but nevertheless unacceptable use is a student computer on the University network running a wildly popular Web server whose content is not Restricted but that ties up the dormitory network. Note that in this case the unacceptable activity running an educationally-irrelevant Web server, which is neither Core nor Restricted, but rather the Web server's interference with others

10 For example, discussion among online participants in a faculty-sponsored, University-hosted discussion group irrelevant to University education or research might become heatedly ad hominem. Participants might ask the University to act against other participants, or to force the faculty sponsor to include or exclude certain participants. Or a third party might take exception to pejorative comments, and, based on the discussion server's location on the University network, institute legal action against the University. The discussion group thus consumes University resources (such as General Counsel time). Because the discussion group is an ancillary use of information technology, its consumption of University resources makes it an unacceptable use of University information technology.

11 To achieve this objective, authorized systems or technical managers occasionally need to examine the contents of particular files to diagnose or solve problems.

12 To achieve this, authorized staff occasionally restrict inequitable use of shared systems or of the network. For example, the University may require users to refrain from using any program that is unduly resource-intensive.

13 Authorized systems administrators occasionally find it necessary to lock a user's account. If the situation is not resolved within 24 hours, the matter goes to the appropriate University officer for follow-up and resolution.

14 Users must establish appropriate passwords, change them occasionally, and never share them with others. Users may not attempt to evade, disable, or "crack" passwords or other security provisions. These activities threaten the work of others and are grounds for immediate disciplinary action. Unauthorized copying of files or passwords belonging to others or to the University may constitute plagiarism or theft. Modifying files without authorization (including altering information, introducing viruses or Trojan horses, or damaging files) is unethical, may be illegal, and can lead to disciplinary action.

15 Users must maintain and archive backup copies of important work. Users are responsible for backing up their own files. They should not assume that files on shared machines are backed up. If users choose to participate in a backup service, they must become familiar with the schedules and procedures of that service. They also must learn to use properly the features for securing or sharing access to their files.

16 In particular, owners or operators of computers on the University network may not grant accounts on their computers or other access to anyone but Regular Users according to the policy definition.

17 The security of electronic files on shared systems and networks is limited. Although most people respect security and privacy mechanisms, they are not foolproof. Electronic mail and other network communications are susceptible to interception absent active steps to protect them, such as encryption.

Georgia Institute of Technology's Acceptable Network Use Policy:

Georgia Tech Network Usage Policy

COMPUTER AND NETWORK USAGE POLICY
"Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, the right to privacy, and the right to determine the form, manner, and terms of publication and distribution. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community."
-
The EDUCOM Code, 1987
http://www.educause.edu/

1. BACKGROUND AND PURPOSE
This document constitutes an Institute-wide policy intended to allow for the proper use of all Georgia Tech computing and network resources, effective protection of individual users, equitable access, and proper management of those resources. This document should be broadly interpreted. This policy applies to Georgia Tech network usage even in situations where it would not apply to the computer(s) in use. These guidelines are intended to supplement, not replace, all existing laws, regulations, agreements, and contracts that currently apply to computing and networking services.
Campus units that operate their own computers or networks are encouraged to add, with the approval of the unit head, individual guidelines that supplement, but do not lessen the intent of this policy. In such cases, the unit will inform users and provide a copy of the unit-level policy to the Office of Information Technology, Information Security Directorate upon implementation.
Access to the Georgia Tech Network is a privilege, not a right. Access to networks and computer systems owned or operated by Georgia Tech requires certain user responsibilities and obligations and is subject to Institute policies and local, state, and federal laws. Appropriate use should always be legal and ethical. Users should reflect academic honesty, mirror community standards, and show consideration and restraint in the consumption of shared resources. Users should also demonstrate respect for intellectual property; ownership of data; system security mechanisms; and individual rights to privacy and to freedom from intimidation, harassment, and annoyance. Appropriate use of computing and networking resources

includes instruction; independent study; authorized research; independent research; communications; and official work of GT units, recognized student and campus organizations, and agencies of the Institute.

2. DEFINITIONS

2.1. Authorized use

Authorized use of Georgia Tech-owned or operated computing and network resources is use consistent with the education, research, and service mission of the Institute, and consistent with this policy.

2.2. Authorized users

Authorized users are (1) current faculty, staff, and students of the Institute; (2) individuals connecting to a public information service (see section 6.5); and (3) others whose access furthers the mission of the Institute and whose usage does not interfere with other authorized users' access to resources. The policy Access by External Entities to Institute Information Technology (and any subsequent revisions) may apply. In addition, a user must be specifically authorized to use a particular computing or network resource by the campus unit responsible for operating the resource.

3. INDIVIDUAL PRIVILEGES

The following individual privileges, all of which currently exist at Georgia Tech, empower all members of the Georgia Tech community to be productive members of that community. It must be understood that privileges are conditioned upon acceptance of the accompanying responsibilities within the guidelines of the Computer and Network Usage Policy.

3.1. Privacy

To the greatest extent possible in a public setting, Georgia Tech seeks to preserve individual privacy. Electronic and other technological methods must not be used to infringe upon privacy. However, Georgia Tech computer systems and networks are public and subject to the Georgia Open Records Act. All content residing on Institute systems is subject to inspection by the Institute.

For information on monitoring network usage and file inspections, please reference section 5.5.

3.1.1. Encryption and password protection

Encryption utilities or password protection schemes requiring data recovery via a password or encryption key may not be used on the Institute's systems without unit-level approval of a recovery process.

3.2. Ownership of intellectual works

Anyone creating intellectual works using Georgia Tech computers or networks, including but not limited to software, should consult Determination of Rights and Equities in Intellectual Property (refer to Board of Regents Policy Manual, section 603.03, 2/2/94 and any subsequent revisions at http://www.usg.edu/admin/policy/600.phtml and related Georgia

Tech policies).

3.3. Freedom from harassment and undesired information

All members of the campus community have the right not to be harassed by computer or network usage by others. (See 4.1.3.)

4. INDIVIDUAL RESPONSIBILITIES

Just as each member of the campus community enjoys certain privileges, so too is each member of the community responsible for his or her actions. The interplay of these privileges and responsibilities engenders the trust and intellectual freedom that form the heart of this community. The trust and freedom that exists are grounded in each person's developing the skills necessary to be an active and contributing member of the community. These skills include awareness and knowledge about information and the technology used to process, store, and transmit it.

4.1. Common courtesy and respect for rights of others

Users are responsible to all other members of the campus community in many ways. They include the responsibility to:

Respect and value the right of privacy,

Recognize and respect the diversity of the population and opinion in the community, and

Comply with Institute policy and all laws and contracts regarding the use of information that is the property of others.

4.1.1. Privacy of information

Files of personal information, including programs, but regardless of storage medium or transmittal, are subject to the Georgia Open Records Act if stored on Georgia Tech's computers (see section 3.1). Nonetheless, individuals are prohibited from looking at, copying, altering, or destroying anyone else's personal files without explicit permission (unless authorized or required to do so by law or regulation). The ability to access a file or other information does not imply permission to do so.

4.1.2. Intellectual property

Users are responsible for recognizing and honoring the intellectual property rights of others.

4.1.3. Harassment

No member of the community may, under any circumstances, use Georgia Tech's computers or networks to harass any other person.

The following constitutes computer harassment: (1) Intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend, or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family; (2) Intentionally using the computer to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not an actual message is communicated, and/or thepurpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease; (3) Intentionally using the computer to contact another person repeatedly regarding a matter for which one does

not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease (such as debt collection); (4) Intentionally using the computer to disrupt or damage the academic, research, administrative, or related pursuits of another; and (5) Intentionally using the computer to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

4.2. Responsible use of resources

Users are responsible for knowing what information resources (including networks) are available, remembering that the members of the community share them, and refraining from all acts that waste or prevent others from using these resources, or from using them in whatever ways have been proscribed by the Institute and the laws of the state and federal governments. Details regarding available resources are available in many ways, including consulting your computing support representative (CSR) (see section 6.4), conferring with other users, examining online and printed references maintained by OIT and others, and visiting the OIT Customer Support Center or its website at http://www.oit.gatech.edu/cs.

4.2.1. Domain Names

Requests to establish new domain names within the Georgia Tech network domain will be forwarded to the Office of Information Technology. Requests for names not ending in "gatech.edu" will not normally be approved. All such requests require the approval of the Associate Vice President and Associate Vice Provost for Information Technology.

4.3. Information Integrity

Each individual is responsible for being aware of the potential for and possible effects of manipulating information, especially in electronic form. Each individual is responsible for understanding the changeable nature of electronically stored information, and to verify the integrity and completeness of information compiled or used. No one should depend on information or communications to be correct when they appear contrary to expectations. It is important to verify that information with the source.

4.4. Use of personally managed systems

Personally managed systems are not limited to computers physically located on the campus, but include any type of device that can be used to access Institute computing and networking resources from any location. Authorized users have a responsibility to ensure the security and integrity of system(s) accessing other computing and network resources of the Institute, whether you are a student, employee, or other authorized user. Institute information electronically stored therein must be protected.

Appropriate precautions for personally owned or managed systems include performing regular backups, controlling physical and network access, using virus protection software, and keeping any software installed (especially anti-virus and operating system software) up to date with respect to security patches. http://www.security.gatech.edu/system_admin.html

Authorized users must ensure compliance with the security, software, and support policies of their unit. The CSR of the unit is an appropriate resource to consult with regarding these policies.

4.5. Access to facilities and information

4.5.1. Sharing of access

Computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others. You are responsible for any use of your account.

4.5.2. Permitting unauthorized access

Authorized users may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users. (See section 2.2.)

4.5.3. Use of privileged access

Access to information should be provided within the context of an authorized user's official capacity with the Institute. Authorized users have a responsibility to ensure the appropriate level of protection over that information.

4.5.4. Termination of access

When an authorized user changes status (e.g., terminates employment, graduates, retires, changes positions or responsibilities within the Institute, etc.), the unit responsible for initiating that change in status must coordinate with the user to ensure that access authorization to all Institute resources is appropriate. An individual may not use facilities, accounts, access codes, privileges, or information for which he/she is not authorized.

4.6. Attempts to circumvent security

Users are prohibited from attempting to circumvent or subvert any system's security measures. This section does not prohibit use of security tools by personnel authorized by OIT or their unit.

4.6.1. Decoding access control information

Users are prohibited from using any computer program or device to intercept or decode passwords or similar access control information.

4.6.2. Denial of service

Deliberate attempts to degrade the performance of a computer system or network or to deprive authorized personnel of resources or access to any Institute computer system or network are prohibited.

4.6.3. Harmful activities

Harmful activities are prohibited. Examples include IP spoofing; creating and propagating viruses; port scanning; disrupting services; damaging files; or intentional destruction of or damage to equipment, software, or data.

4.6.4. Unauthorized access

Authorized users may not:

Damage computer systems

Obtain extra resources not authorized to them

Deprive another user of authorized resources

Gain unauthorized access to systems by using knowledge of:

A special password
Loopholes in computer security systems
Another user's password
Access abilities used during a previous position at the Institute

4.6.5. Unauthorized monitoring

Authorized users may not use computing resources for unauthorized monitoring of electronic communications.

4.7. Academic dishonesty

Authorized users should always use computing resources in accordance with the high ethical standards of the Institute community. Academic dishonesty is a violation of those standards, including the Academic Honor Code. http://www.honor.gatech.edu

4.8. Use of copyrighted information and materials

Users are prohibited from using, inspecting, copying, storing, and redistributing copyrighted computer programs and other material, in violation of copyright laws.

4.9. Use of licensed software

No software may be installed, copied, or used on Institute resources except as permitted by the owner of the software. Software subject to licensing must be properly licensed and all license provisions (installation, use, copying, number of simultaneous users, term of license, etc.) must be strictly adhered to.

4.10. Political campaigning; commercial advertising

Please refer to Board of Regents Policy (Section 914.01) - http://www.usg.edu/admin/policy/900.phtml
Georgia Tech Faculty Handbook (Section 6.15.3.8(b)) - http://dept.gatech.edu/handbook/Section6/Facility.html

4.11. Personal business

Computing facilities, services, and networks may not be used in connection with compensated outside work nor for the benefit of organizations not related to Georgia Tech, except in accordance with the Institute Consulting Policy or the policy Access by External Entities to Institute Information Technology Resources. State law restricts the use of state facilities for personal gain or benefit.

5. GEORGIA TECH PRIVILEGES

Our society depends on institutions such as Georgia Tech to educate our citizens and advance the development of knowledge. However, in order to survive, Georgia Tech must attract and responsibly manage financial and human resources. Therefore, Tech has been granted by the state, and the various other institutions with which it deals, certain privileges regarding the information necessary to accomplish its goals and to protect the equipment and physical assets used in its mission.

5.1. Allocation of resources

Georgia Tech may allocate resources in differential ways in order to

achieve its overall mission.

5.2. Control of access to information

Georgia Tech may control access to its information and the devices on which it is stored, manipulated, and transmitted, in accordance with the laws of Georgia and the United States and the policies of the Institute and the Board of Regents.

5.3. Imposition of sanctions

Georgia Tech may impose sanctions and punishments on anyone who violates the policies of the Institute regarding computer and network usage.

5.4. System administration access

A system administrator (i.e., the person responsible for the technical operations of a particular machine) may access others files for the maintenance of networks and computer and storage systems, such as to create backup copies of media. However, in all cases, all individuals' privileges and rights of privacy are to be preserved to the greatest extent possible.

5.5. Monitoring of usage, inspection of files

Users should also be aware that their uses of Georgia Tech's computing resources are not completely private. While the Institute does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the Institute's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for maintaining network availability and performance.

The Institute may also specifically monitor the activity and accounts of individual users of the Institute's computing resources, including individual login sessions and communications, without notice. This monitoring may occur in the following instances:

- The user has voluntarily made them accessible to the public.
- It reasonably appears necessary to do so to protect the integrity, security, or functionality of the Institute or to protect the Institute from liability.
- There is reasonable cause to believe that the user has violated, or is violating, this policy.
- An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns.
- Upon receipt of a legally served directive of appropriate law enforcement agencies.

Any such individual monitoring, other than that specified in "(1)", required by law, or necessary to respond to bona fide emergency situations, must be authorized in advance by the Office of Legal Affairs and the Associate Vice President and Associate Vice Provost for Information Technology; in all such cases, the appropriate unit head will be informed as time and the situation will allow. In all cases, all

individuals' privileges and right of privacy are to be preserved to the greatest extent possible.
For further information, please see 3.1 for information on privacy.

5.6. Suspension of individual privileges

Units of Georgia Tech operating computers and networks may suspend computer and network privileges of an individual for reasons relating to his/her physical or emotional safety and well-being, or for reasons relating to the safety and well-being of other members of the campus community, or Institute property. Access will be promptly restored when safety and well-being can be reasonably assured, unless access is to remain suspended as a result of formal disciplinary action imposed by the Office of the Vice President for Student Affairs (for students) or the employee's department in consultation with the Office of Human Resources (for employees).

6. GEORGIA TECH RESPONSIBILITIES

6.1. Risk management

Georgia Tech, through the Department of Internal Auditing, maintains a periodic risk evaluation process to protect its information systems infrastructure and data in the face of a changing information security environment. All unit heads are required to approve an annual risk evaluation conducted by the unit with a semi-annual follow-up on identified risks.
Benefits of a properly performed risk analysis include:

- Increase security awareness at all organizational levels from operations to management.
- Evaluate the status of the current security posture.
- Highlight areas where greater security is needed.
- Assemble facts, dispel myths, and fight complacency.
- Justify, prioritize,and implement effective counter-measures and procedures.

These evaluations will entail a thorough review of each unit's information security policy, procedures, and practices. The current evaluation procedure is posted at:

http://www.audit.gatech.edu/ia/prod03.htm.

The aggregate of Unit Information Systems Risk Evaluations will be based on results from the Unit Risk Evaluations collected by the OIT Information Security Directorate and assembled with collaboration from Internal Auditing. The results and recommendations will be submitted to the President's Office semi-annually.
Units will develop a policy for purchasing computing resources to ensure these resources fit the unit's technology architecture and are properly supported.

6.2. Security procedures

Georgia Tech has the responsibility to develop, implement, maintain, and enforce appropriate security procedures to ensure the integrity of

individual and institutional information, and to impose appropriate penalties when privacy is purposefully abridged.

6.3. Anti-harassment procedures

Georgia Tech has the responsibility to develop, implement, maintain, and enforce appropriate procedures to discourage harassment through the use of its computers or networks and to impose appropriate penalties when such harassment takes place. Georgia Tech's anti-harassment policy and procedures are available at:
http://www.admin-fin.gatech.edu/business/human/relations/070500.html

6.4. Upholding of copyrights and license provisions

Georgia Tech has the responsibility to uphold all copyrights, laws governing access and use of information, and rules or contractual requirements of organizations supplying information resources to members of the community (e.g., Internet acceptable use policies and license requirements for commercial information databases). The Georgia Tech Library maintains copies of relevant copyright laws and guidelines at:
http://www.library.gatech.edu/resvcopyright_frame.htm

6.5. Individual unit responsibilities

Each unit is responsible for compliance with Section 6. Units are to designate a computing support representative (CSR)and notify the director of Customer Support, Office of Information Technology, of CSR appointments. CSRs will be knowledgeable about their units' computing environment and central resources and services. Units are responsible for compliance with risk evaluation procedures and the General Prevention Measures. CSRs are the first point of contact for unit personnel seeking problem resolution, information, and other assistance regarding computing and networking. CSRs will facilitate interaction between the unit and the Office of Information Technology and Internal Auditing regarding security issues.
Risk evaluation procedures: http://www.audit.gatech.edu/ia/prod03.htm.
General Prevention Measures:
http://www.security.gatech.edu/policy/general_measures.html

6.6. Public information services

Units and individuals may, with the permission of the appropriate unit head, configure computing systems to provide information retrieval services to the public at large. (Current examples include "ftp" and "www.") However, in so doing, particular attention must be paid to the following sections of this policy: 2.1 (authorized use [must be consistent with Institute mission]), 3.3 (ownership of intellectual works), 4.2 (responsible use of resources), 4.9 (use of copyrighted information and materials), 4.10 (use of licensed software), and 6.4 (individual unit responsibilities). Use of public services must not cause computer or network loading that impairs other services or impedes access by authorized users.

7. PROCEDURES AND SANCTIONS

7.1. Investigative contact

If anyone is contacted by a representative from an external law enforcement organization (District Attorney's Office, FBI, GBI, ISP security officials, etc.) that is conducting an investigation of an alleged violation involving Georgia Tech computing and networking resources, they must inform the OIT Information Security Directorate at http://www.security.gatech.edu/ and the Georgia Tech Office of Legal Affairs, 404-894-4812, immediately. Refer the requesting agency to the Associate Vice President and Associate Vice Provost for Information Technology; that Office will provide guidance regarding the appropriate actions to be taken. For routine matters, send e-mail to security@gatech.edu. For urgent matters, contact OIT Operations at 404-894-4669 and someone from the OIT Information Security Directorate will be paged immediately.

7.2. Responding to security and abuse incidents

All authorized users are stakeholders and share a measure of responsibility in intrusion detection, prevention, and response. At Georgia Tech the Associate Vice President and Associate Vice Provost for Information Technology has been delegated the authority to enforce information security policies and is charged with:

- Implementing system architecture mandates, system protection features, and procedural information security measures to minimize the potential for fraud, misappropriation, unauthorized disclosure, loss of data, or misuse.
- Initiating appropriate and swift action, using any reasonable means, in cases of suspected or alleged information security incidents to ensure necessary protection of Institutes resources, which may include disconnection of resources, appropriate measures to secure evidence to support the investigation of incidents, or any reasonable action deemed appropriate to the situation.

All users and units have the responsibility to report any discovered unauthorized access attempts or other improper usage of Georgia Tech computers, networks, or other information processing equipment. If you observe, or have reported to you (other than as in 7.1 above), a security or abuse problem with any Institute computer or network facilities, including violations of this policy:

Take immediate steps as necessary to ensure the safety and well-being of information resources. For example, if warranted, a system administrator should be contacted to temporarily disable any offending or apparently compromised computer accounts, or to temporarily disconnect or block offending computers from the network (see section 5.6).

Ensure that the following people are notified: (1) your computing support representative, (2) your unit head, and (3) the OIT Information Security Directorate.

The OIT Information Security Directorate will coordinate the technical and

administrative response to such incidents. Reports of all incidents will be forwarded to Student Affairs (for apparent policy violations by students) or the unit head (for employees), and to the Associate Vice President and Associate Vice Provost for Information Technology.

7.3. First and minor incident

If a person appears to have violated this policy, and (1) the violation is deemed minor by OIT, and (2) the person has not been implicated in prior incidents, then the incident may be dealt with at the unit level. The alleged offender will be furnished a copy of the Institute Computer and Network Usage Policy (this document) and will sign a form agreeing to conform to the policy.

7.4. Subsequent and/or major violations

Reports of subsequent or major violations will be forwarded to Student Affairs (for students) or the unit head (for employees) for investigation and appropriate action. Units should consult the Office of Human Resources regarding appropriate action.

7.5. Range of disciplinary sanctions

Persons in violation of this policy are subject to the full range of sanctions, including the loss of computer or network access privileges, disciplinary action, dismissal from the Institute, and legal action. Some violations may constitute criminal offenses, as outlined in the Georgia Computer Systems Protection Act and other local, state, and federal laws; the Institute will carry out its responsibility to report such violations to the appropriate authorities.

7.6. Appeals

Appeals should be directed through the existing procedures established for employees and students.

7.7. Links to applicable policies and procedures:

Local, state, and federal laws - http://www.security.gatech.edu/policy/law_library.html

Incident Response Guidelines - http://www.security.gatech.edu

General Prevention Measures - http://www.security.gatech.edu/policy/general_measures.html

OHR Policies and Procedures - http://www.admin-fin.gatech.edu/business/human/

Institute Consulting Policy or the policy Access by External Entities to Institute Information Technology Resources - http://www.security.gatech.edu/policy/xaccess.html

Determination of Rights and Equities in Intellectual Property (Board of Regents Policy Manual, section 603.03) - http://www.usg.edu/admin/policy/600.phtml - 603.03 - http://www.usg.edu/admin/policy/

OIT Customer Support Center - http://www.oit.gatech.edu/cs

Georgia Tech Faculty Handbook (section 6.15.3.8(b) - http://www.ohr.gatech.edu/policies/handbook.pdf

Georgia Tech Academic Honor Code - http://www.honor.gatech.edu

Board of Regents Policy Manual (Use of System Materials) - http://www.usg.edu/admin/policy/900.phtml

Emory University Acceptable Network Use Policy:

Information Technology Policies

Policies, Guidelines, and Laws

Information Technology Use Policy

10 October 1994

Electronic Information Technology Systems at Emory University are essential and indispensable tools for learning, research and administration. It is the policy of the University that its computing, telecommunications, video, and associated network facilities be used ethically and legally, in accord with applicable licenses and contracts, and according to their intended use in support of the University's mission.

Any use that would impede teaching and research, hinder the functioning of the University, violate an applicable license or contract, or damage community relations or relations with institutions with whom we share responsibility, is a violation of this policy.

Violation of this policy may result in suspension of privileges to access the information technology involved, initiation of University disciplinary procedures or, in extreme cases, criminal prosecution under federal or state law.

Please refer any questions about this policy or its applicability to a particular situation to the Vice-Provost for Information Technology.

Policy Background and History

This policy is the result of bringing together the gist of policies of several institutions (indicated below). Because much of the existing material did not reflect current thinking or technology, this policy includes many concepts and issues not found in those policies. Most of the existing material was not generalized, i.e. it contained references to University specific situations, facilities and technology. Many were written from the point of view of the classic "Computer Center". This policy is written from a university point of view. It is assumed that the University computing environment is a collection of separately administrated local area networks (including local servers, printers etc.), departmental and central servers most of which are attached to a University backbone network. The backbone network provides dial-in access and access to external national and international networks. During the course of policy development, the scope of Information Technology was expanded to include voice and video.

This policy was originated in the Academic Computing Advisory Committee and reviewed through twelve drafts by a wide audience, including University

Counsel over a period of nearly two years. My thanks to all the reviewers. I don't believe a single sentence escaped unscathed. It's the same axe, only the handle and blade have been replaced. However, as someone once said, "We have not succeeded in answering all your questions. The answers we have found only serve to raise a whole set of new questions. In some ways we feel we are as confused as ever, but we believe we are confused on a higher level and about more important things".
Larry Frederick

This policy was strongly influenced by the policies of the following institutions:

Baylor University
Boston University
Columbia University
Daniel Webster College
James Madison University
Lehigh University
MIT (Project Athena)
Purdue University
Research Institute for Advanced Computer Science
State of Wisconsin Statutes on Computer Crime
Stevens Institute of Technology
University of California Irvine
University of Idaho
University of New Mexico
University of Missouri-Columbia
University of Missouri-Kansas City
University of Missouri-Rolla
University of Pittsburgh
Washington University

This policy was also influenced by the following policies:

CREN (BITNET) Acceptable Use Policy
EARN Charter and Use
Emory University Draft E-Mail Use
EUIT project, Dilemmas in the Ethical Use of Information Technologies: A Resource Kit
EUIT project, Dilemmas in Ethical Uses of Information, October 1992 draft of

The Bill of Rights and Responsibilities for Electronic Learners.

© Emory University
Last Update: Tuesday, June 27 2000

Harvey Mudd College Acceptable Network Use Policy:

A. Appropriate Use of Campus Computing and Network Resources

Harvey Mudd College makes available computing and network resources which may be used by College students, faculty and staff. These are intended to be used for educational purposes and to carry out the legitimate business of the College. Appropriate use of the resources includes instruction, independent study, authorized research, independent research, and the official work of the campus organizations and agencies of the College. The computing and network resources of the College may not be used by members of the College community for commercial purposes without the explicit approval of the Director of Computing and Information Services, the Harvey Mudd College Computing Committee, or the Harvey Mudd College Treasurer.

The privilege of using the campus and network computing resources provided by the College is not transferable or extendible by members of the College community to people or groups outside the College without the explicit approval of the Director of Computing and Information Services or the Harvey Mudd College Computing Committee.

Those who avail themselves of the computing and network resources are required to behave in their use of the technology in a manner consistent with the College's Standards of Conduct. For example, as stated in the Harvey Mudd College Catalogue:

"When students enter Harvey Mudd College, it is assumed that they have an earnest purpose. Students are expected to act as responsible individuals, to conduct themselves with honesty and integrity both personally and academically, and to respect the rights of others..."

Similar expectations are held for other members of the college community.

The College has subscribed to the statement on software and intellectual rights distributed by EDUCOM, the non-profit consortium of colleges and universities committed to the use and management of information technology in higher education, and ITAA, the Information Technology Association of America, a computer software and services industry association:

"Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to work of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and right to determine the form, manner, and terms of publication and distribution."

"Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community."

The framework of responsible, considerate, and ethical behavior expected by the College extends to cover the use of campus microcomputers and workstations, departmental computing facilities, general-use computers, campus network resources, and networks throughout the world to which the College provides computer access. The following list does not cover every situation which pertains to proper or improper use of the resources, but it does suggest some of the responsibilities which you accept if you choose to use a College computing resource or the network access which the College provides.

1. For any computer account, you are responsible for the use made of that account. You should set a password which will protect your account from unauthorized use, and which will not be guessed easily. If you discover that someone has made unauthorized use of your account, you should change the password and report the intrusion to the manager of that system or the Director of Computing and Information Services. You should change your password on a regular basis, to assure continued security of your account.
2. You must not intentionally seek information about, browse, copy, or modify files or passwords belonging to other people, whether at Harvey Mudd or elsewhere, unless specifically authorized to do so by those individuals. If an individual has explicitly and intentionally established a public server, or clearly designated a set of files as being for shared public use, others may assume authorization. However, if it is unclear whether some files are intended to be available for public use or not, you should assume that they are private files and are not intended for public access.
3. You must not attempt to decrypt or translate encrypted material, or obtain system privileges to which you are not entitled. You must refrain from any action which interferes with the supervisory or accounting functions of the systems or that is likely to have such effects. If you encounter or observe a gap in system or network security, you must report the gap to the manager of that system or the Director of Computing and Information Services.
4. You must be sensitive to the public nature of shared facilities, and take care not to display on screens in such locations images, sounds or messages that could create an atmosphere of discomfort or harassment for others. You must also refrain from transmitting to others in any location inappropriate images, sounds or messages which might reasonably be considered harassing. The College's policies on harassment apply equally to electronic displays and communications as they do to more traditional means of display and communication.
5. You must avoid wasting computing resources by excessive game playing or other trivial applications; by sending chain letters or other frivolous or excessive messages locally or over an attached network; by printing excessive copies of documents, files, images, or data. You must refrain from using unwarranted or excessive amounts of storage; printing documents of files numerous times because you have not checked thoroughly for all errors and corrections; or running grossly inefficient programs when efficient ones are available. You must be sensitive to the specialized nature of software, hardware, and services available in a limited number of locations, and allow access to those people whose work requires these specialized facilities.
6. You must not prevent others from using shared resources by running unattended processes or placing signs on devices to "reserve" them without authorization from the appropriate system manager. Your absence from a public computer or workstation should be no longer than warranted by a visit to the nearest rest room. A device unattended for more than ten minutes may be assumed to be available for use, and any process running on that device terminated. You must also be sensitive to performance effects of remote login to shared workstations: when

there is a conflict, priority for use of the device must go to the person seated at the workstation rather than to someone logged on remotely.

7. The College presents for your use many programs and data which have been obtained under contracts or licenses saying they may be used but not copied, cross-assembled, or reverse-compiled. In addition, other institutions and individuals on attached networks make software available under similar conditions. You are responsible for determining that programs or data are not restricted in this manner before copying them in any form, or before reverse-assembling or reverse-compiling them in whole or in any part. If it is unclear whether you have permission to copy such software or not, assume that you may not do so.
8. If you create or maintain electronically-stored data which is important to your work or to the College in general, you are responsible for the backup of that data. The College does backup data on its general access systems at regular intervals as preparation for a catastrophic loss of resources. However, you must decide whether or not this is an adequate substitute for making your own backups of the data you create or maintain.
9. Messages, sentiments, and declarations sent as electronic mail or sent as electronic postings must meet the same standards for distribution or display as if they were tangible documents or instruments. You are free and encouraged to publish your opinions, but they must be clearly and accurately identified as coming from you; or if you are acting as the authorized agent of a group, they must be identified as coming from that group. You must not falsely attribute (i.e. forge) the origin of electronic mail, messages, or postings. If you create, alter, or delete any electronic information contained in, or posted to any campus computer resource or to any computer resource on an attached network it will be considered forgery if it would be considered so on a tangible document or instrument.
10. You must not create or willfully disseminate computer viruses. You should be sensitive to the ease of spreading viruses and should take steps to insure your files are virus free.

Again, the above are only examples and not an exhaustive list. You also should be aware that there are Federal, State and sometimes local laws which govern certain aspects of computer and telecommunications use. Members of the College community are expected to respect these laws, as well as to observe and respect College rules and regulations.
In the normal course of operating and maintaining the network and the systems connected to it, the contents of files and of data on the network will not be examined without authorization, except by accident. When there is reason to suspect inappropriate use of campus computing or networking resources, the Director of Computing and Information Services will authorize specific College personnel to take steps to investigate. This may include monitoring traffic on the network, including its contents, and examining files on any system that has connected to the HMC network. The Director of Computing and Information Services will report any such actions to the HMC Computing Committee during the next regular working day.
For students, violations of appropriate use may result in one or more of the following actions:

1. A written warning to the offender.
2. A restriction of system access for a specified term.
3. A revocation of all system privileges for a specified term.
4. A statement of charges to the appropriate disciplinary body at the student's home college, which could lead to other penalties up to and including probation or suspension.

The following procedures are intended to maintain orderly operation of the system while providing due process for anyone charged with misusing it:

1. A user who is directed by an Computing and Information Services employee to cease engaging in any computing or network related activity must do so.
2. The Director of Computing and Information Services must review any such action during the next regular working day, and either restore privileges or send a written statement of charges to the Dean of Faculty at HMC.

If you have questions about the "Appropriate Use" of computer resources and networks at Harvey Mudd College, you should contact either the Director of Computing and Information Services or a member of the Harvey Mudd College Computing Committee.

Pitzer College Acceptable Network Use Policy:

Residential Networking User Agreement
Information Technology
Policies and Procedures
Computer Facilities
Residential Networking
Media Studies
Audio Visual
Meet our Staff
Documentation

Use of your computer accounts, Pitzer Network access and their services is a privilege. By installing the Residential Networking software and/or connecting your computer to the Pitzer College Network in any way, you have agreed to obey the rules and policies of the Pitzer Computing Department. All users of Pitzer Network resources are bound to federal, state, and local laws. Failure to follow any and all of these rules may result in the loss of this privilege.

Users of any of the Pitzer College computer resources will follow all general lab rules.

Each user is assigned an individual account. Users will use this account only. Users will be expected to show some form of identification when acquiring their account.

The user is responsible for choosing a password during his/her first session, and for maintaining its security. Passwords must be changed every six (6) months, or as required by the system.

The computer accounts of other users are private. Users who are caught snooping in or copying from other user's files without the other person's permission may lose their system privileges.

Users misrepresenting themselves while using any of Pitzer's computer resources will not be tolerated. This refers especially to sending e-mail messages using a falsified name or someone else's account.

No unauthorized use of the computer network will be tolerated. This includes, but is not limited to attempting to break into other systems and creating and/or disseminating computer viruses.

ANY process which might result in a loss of effectiveness or possible server malfunction should first be cleared with a Computing Staff member before attempting to execute the program.

ANY changes to the content or configurations of any system or computer, with the exception of the user's personal computer, MUST first be cleared with a Computing Staff member. This includes adding and running any programs outside of the established computer lab catalog (i.e. games).

Violation of copyright laws will not be tolerated. Copyrighted material will be removed from Pitzer owned machines, this includes images and software that is not licensed.

Any complaints regarding a user should be forwarded via Email to Help@Pitzer.edu.

Users are not permitted to let friends and/or relatives use their accounts.

No commercial use of any computing service is allowed. No sales are to be made or advertised. No fees are to be charged for use of any Pitzer Network access.

Computer resources may not be used to engage in abuse of other users, such as sending abusive or obscene messages within or beyond Pitzer via the network.

Users are responsible for their own data. All files should be saved either to the user's hard drive, a diskette, or the user's home directory. Any files that are NOT saved in a user's home directory or to floppy disk are subject to erasure. The server will be cleaned out on a regular basis. Files saved on a student's personal computer are exempt from erasure.

Abusive or improper use of any Pitzer computer resources is not allowed. This includes, but is not limited to, misuse of the system-operator privilege, tampering with equipment, unauthorized attempts at repairing equipment, and unauthorized removal of equipment components.

Users who wish to use their computers to provide services to persons outside Pitzer via the Pitzer Network are bound to the policies of the Pitzer Network Service Provider Agreement

Note: Loss of the computing privilege includes, but is not limited to, deactivation of all accounts and removal of the user's network connection.

Pitzer Network Service Provider Agreement

Any person who attaches their computer to the Pitzer Network and configures that computer to provide any service to persons outside Pitzer are bound to the following regulations. Any violation of these regulations could result in the loss of the computing privilege.

Once a student connects their computer to the Pitzer Network and configures that computer to provide any service to persons outside Pitzer via the Pitzer Network, that student becomes a Service Provider. As a Service Provider, the student is responsible for the actions and conduct of anyone who uses their service.

All regulations stated in the Pitzer Residential Networking User Agreement are to be observed by all users of the Service Provider's services.

The Service Provider provides services at their own risk. No support, outside that given to any other student, will be given.

Many portions of the Pitzer Network are public (i.e. Web sites) and should be administered accordingly. Offensive and/or abusive material will not be tolerated.

Service Providers are not to allow access to the Pitzer Network to anyone who violates or otherwise does not meet the requirements of the Pitzer Residential Networking User Agreement.

No commercial use of any computing service is allowed. No sales are to be made or advertised. No fees are to be charged for use of any Pitzer Network access.

Note: Loss of the computing privilege includes, but is not limited to, deactivation of all accounts, removal of the user's network connection, disciplinary action, and/or legal action.

Send questions and comments regarding this site to webmaster@pitzer.edu

Bibliography

[1] Napster, Inc.
<http://www.napster.com>
[2] William F. Massy, *Computer Networks: Making the Decision to Join One*
, Science: New Series, Vol. 186, No. 4162, p. 414 (1974)
[3] Michael Hauben, "The Social Forces Behind the Development of Usenet"
Netizens: An Anthology (1996)
<http://www.columbia.edu/~rh120/ch106.x03>
[4] Linnda R. Caporael, *College Students' Computer Use*
Journal of Higher Education (1985) Ohio State University Press
[5] *About Internet2*
University Corporation for Advanced Internet Development (2001)
<http://www.internet2.edu/html/about.html>
[6] Gregory A. Jackson, *Evaluating Learning Technology: Methods, Strategies, and Examples in Higher Education*
Journal of Higher Education, Vol. 61, No. 3 (May/June 1990) Ohio State University Press
[7] John P. Walsh, *Self-Selected and Randomly Selected Respondents in a Computer Network Survey*
Public Opinion Quarterly (1992) University of Chicago Press
[8] Erdman, Harold P., Marjorie H. Klein, and John H. Greist, *Direct Patient Computer Interviewing*
Journal of Counseling and Clinical Psychology 53:76-73. (1985)
[9] *H.R.2281, Digital Millennium Copyright Act (Enrolled Bill)*
<http://thomas.loc.gov/cgi-bin/query/z?c105:H.R.2281.ENR:>
[10] Lucash Gesmer & Updegrove, *Massachusetts Computer Crime Bill* (April 1993)
<http://www.lgu.com/publications/ecommerce/99.shtml>
[11] *What is Gnutella?*
Gnutella News (2001)
<http://www.gnutellanews.com/information/what_is_gnutella.shtml>
[12] Sam Costello, *Universities Refuse to Ban Napster*
IDG News Service\Boston Bureau (September, 2000)
<http://www.idg.net/idgns/2000/09/22/UniversitiesRefuseToBanNapster.shtml>
[13] Heidi Pearlman Salow, *Liability Immunity for Internet Service Providers--How Is It Working?*,
6.1 J. TECH. L. & POL'Y 1
<http://grove.ufl.edu/~techlaw/vol6/Pearlman.html> (2000).
[14] The Harvard Crimson
<http://www.thecrimson.com/>
[15] Worcester Polytechnic Institute Acceptable Network Use Policy
Worcester Polytechnic Institute (2001)
<http://www.wpi.edu/+AUP>
[16] Policy on Appropriate Use of Clark's Computing Resources
Clark University (2001)
<http://www.clarku.edu/offices/ois/computerpolicy.html>
[17] Computer Use Policy
IIT Webgroup (2001)
<http://cns.iit.edu/html/policies/PCompUse.html>
[18] Eligibility and Acceptable Use Policy for Information Technology
University of Chicago (2000)
<http://www.uchicago.edu/docs/policies/eaup/>
[19] Computer and Network Use Policy
Georgia Institute of Technology (2001)
<http://www.itis.gatech.edu/policy/usage/contents.html>
[20] Information Technology Use Policy

Emory University (2000)
<http://www.emory.edu/ITD/POLICY/>
[21] Appropriate Use of Campus Computing and Network Resources
Harvey Mudd College (1998)
<http://www.hmc.edu/comp/policy/appropriate-use.html>
[22] Residential Networking User Agreement
Pitzer College (2000)
<http://www.pitzer.edu/resources/info%5Ftech/resnet/policies.html>
[23]*America's Best Colleges* 2002
U.S.News & World Report Inc. (2001)
<http://www.usnews.com/usnews/edu/college/rankings/rankindex.htm>
[24] *Maximizing Survey Responses*
CustomInsight, Inc.
<http://customer-satisfaction-surveys.custominsight.com/maximize.html>
[25] *Women, Minorities, and Persons With Disabilities in Science and Engineering*
National Science Foundation, (1998) (NSF 99-338)
[26] *Netcraft Web Server Survey*
Netcraft (2001)
<http://www.netcraft.com/survey/>