Chapter 6
Resolving Information Technology Policy Issues
on the Networked Campus

Tracy Mitrano

Organizing and Managing Information
Resources on Your Campus

Polley Ann McClure, Editor

A Publication of EDUCAUSE
Policy is important (McClure, 1998). Policies and policy development have assumed an increasingly central role in higher education for three principal reasons: (1) policy (or lack thereof) is often related to legal liability; (2) the complex structure of academic administration requires explicit operating manuals; and (3) multifaceted and complicated relationships continue to emerge between academic institutions and government and the market. Thus, it is now common for most colleges and universities to support a compendium of policies ranging from a campus code of conduct to environmental health and safety regulations to matters of budget and finance, human resources, legal governance, and information technologies.

The larger the institution is, the more likely it is to support a comprehensive library of policies, but it is important to note that no one-size-fits-all policy, or policy development process, exists. Policies and the policy development process should always strive to embody the traditions, culture, and personality of an institution while serving the special mission of higher education overall.

I thank Steve McDonald, whose work has always been an inspiration, for his guidance in shaping and reviewing this chapter.
The Special Role of Information Technology Policy

In an era in which technology has captured the imagination of higher education and become critical to day-to-day campus communications and operations, information technology (IT) policies have assumed a preeminent role in the overall policy development of colleges and universities. All constituencies want and need to know the rules of the road for appropriate use, maximum efficiency, and heightened security of IT resources. But because these resources are relatively new and, depending on one’s perspective, either exciting or formidable—or both—in their potential for changing research, teaching, and administration, it is tempting to subsume under the IT policy purview administrative policies or functions that do not properly belong there.

For example, electronic communications can be readily used for assault, but assault does not begin and end with a computer. Images of non-obscene adult pornography on a computer screen, while not illegal or, on most campuses, even a violation of policy, may nonetheless contribute to a hostile workplace in certain circumstances. Likewise, an employee may spend five hours a day glued to Internet pornographic images, or use the university computer and network to run a business, or download voluminous amounts of digital material on her favorite hobby, or file-share copyright-protected materials for which he does not have permission. The list of hypothetical problems goes on, but the lesson is clear: policy advisers for information technologies should take special care not to overextend the bounds of their jurisdiction. The ubiquity of computers and network systems does not mean that every behavior that transpires on them is an IT policy issue. Institutions should avoid creating new IT policies when and where it would be more prudent to focus efforts on applying an existing body of policies to the IT environment.

Thus, in the hypothetical case about the employee who exhibits computer images of pornography on his or her office computer, creating a potentially hostile work environment, it makes more sense
to have the human resource department initiate a careful process of progressive investigation into the matter rather than to jump right into the monitoring of electronic communications; otherwise, the institution might run the risk of creating a debate about privacy in the midst of a potentially serious sexual harassment investigation.

Similarly, the excessive use of institutional resources should not be limited to or singularly highlight the electronic medium. Nevertheless, it may be not merely a good idea, but part of a compliance package, to maintain a specific IT policy on resolution of notices on copyright infringement or software piracy. Although intellectual property agreements do not uniquely fall under the purview of IT, developments such as distance learning often initiate discussion, review, and revision of existing policies. Both the insight that central IT administrators bring to those discussions and the investment they have in promoting teaching, learning, and technology projects necessitate that they play a significant role in such discussions. Thus, distinguishing those boundaries is a critical exercise. It keeps IT policies lean and to the point while maintaining mutually beneficial relationships with the associated offices with which policy officers work, such as legal counsel, judicial administrators, human resources, police, and auditors.

This chapter examines the work that needs to be done in the area of IT policy development. For institutions that already have existing policy in this area, guidelines and resources for updating policies are offered.

**Policy Development and Management**

An appreciation of policy requires an understanding of at least the broad outlines of the policy process. Three models for policy development and management stand out: the centralized policy development office model, the decentralized model, and the hybrid model.

In the centralized model, the highest leaders of the institution—that is, the president or provost—authorize a specific policy office
to be the central repository of campus policy and to deploy its personnel in the service of executing a uniform procedure for formulating and issuing policy. Critical to this office is a set of criteria that qualifies a policy for centralized development (such as application of the policy to the institution overall) as a means of distinguishing institution-wide policies from department or local ones. The template for formulating and issuing institutional policies generally includes a policy statement, the reason for the policy, information about to whom (campuses, offices) the policy applies or whom the policy is specifically intended to affect (particular constituencies), and the approximate combination of background information, policy specifics, procedures, responsibilities, and reporting structures. (For an illustration of a policy on formulation and issuance of policies, see www.univco.cornell.edu/policy/pop.for.html.) Creating standing committees with representatives from offices and constituencies around campus that are specifically focused on IT, and even a Web site devoted to policy developments, can assist in the review and communication of policies.

Perhaps not coincidentally, large, decentralized universities seem to gravitate toward this centralized model, probably as a counterbalance to their own decentralized administrative structures. Cornell University and the University of Minnesota are two such examples (see www.univco.cornell.edu/policy/home.html and www.fpd.finop.umn.edu).

Conversely, an institution with a strong central administration, such as Georgetown University, does not appear to require a centralized policy office. Policy development in the decentralized model is instead left to the individual departments or units, with the underlying understanding that should a conflict between them emerge, a robust and authoritative administration will act as the arbiter of the dispute.

Most institutions use a hybrid model in which some aspects of policy development are centralized and others are not. Some colleges
and universities may employ a select group of administrators or constituent representatives to vet policy, but may not have formalized either that membership or the process by which the vetting occurs. Other large universities, for example, Kansas and Michigan, do not have a central policy office but do issue university-wide policies under the authority of the president, provost, or key members of the central administration (see www.ku.edu/~vcinfo/IT_policy/index.htm and www.umich.edu/~policies/). The “marbling” of policy in operations and service agreements is yet another variation, one notably deployed by the Massachusetts Institute of Technology.

The ubiquitous role that information technologies play in higher education makes these distinctions among models for policy development significant. From the start, IT professionals, particularly IT policy advisers, must align with the administrative forces that will inevitably have an impact not only on policy principles but also on process, formulation, and promulgation. In addition to working out the calculus of policy development in general, a policy adviser must weigh the application of a particular policy to the central organization or to the entire distributed network. Institutional size, architecture, and culture as separate issues, as well as taken together, are often important additional considerations (Vernon, Mitrano, and Poulsen, 2002).

The First Generation of IT Policy: Acceptable Use

Acceptable (or responsible or appropriate) use policies were among the first kinds of IT policies to emerge in the late 1980s and early 1990s. An acceptable-use policy generally set some basic ground rules for the use of computers and network systems and often included in one comprehensive policy a multitude of issues that today are more likely to be addressed in distinct policies, for example, security (“no sharing of passwords”), privacy (“the university does not monitor electronic communications as a routine practice”),
data retention ("the central computing organization shall retain logs for six months"), and responsible use ("no violations of law or policy").

The broad frameworks of such policies served to educate the community and bring together many distinct campus constituencies (Graves, Jenkins, and Parker, 1995). These policies gained considerable recognition on campuses throughout the 1990s and continue to provide a necessary foundation for all other IT policy development.

Around this same time, individuals charged with IT policy coordination started to seek each other out and engage in discussions of related policies and practices. Guidelines and considerations for developing IT policy began to appear in professional publications. In the mid-1990s, Stager, Rezmierski, and Pinkerton (1996) offered a comprehensive overview of the policy environment in colleges and universities, identifying emerging policy challenges related to e-mail, digital signatures, racial electronic terrorism, institutional records in an electronic environment, handling of personal information, and libel. Their work identified a set of enduring principles to help clarify issues as belonging to a continuum of campus values. Hodges and Worona (1996), then codirectors of the Computer Policy and Law (CPL) Program at Cornell University, examined the legal underpinnings for creating campus policy, focusing on five common policy areas: adult material, harassment, privacy, commerce, and copyright.

What accounts for the success of these early efforts to develop IT policy about acceptable use of information resources and technologies in the complicated landscape of higher education?

First, they often emerged in tandem with the creation of centralized campus policy offices or policy development initiatives, regardless of model. Once again, the symbiotic relationship between policy development in general and IT policies in particular is worth noting. As networks crossed colleges and universities, their very functionality presented the question of institution-wide policy in order to maintain the security, manageability, and appropriateness of their use. In turn, colleges and universities began to recognize the
need, if not the value, of institution-wide policies to make their rules and regulations uniform, compact, and identifiable.

Second, experience was in many ways the mother of invention. As users of college and university networks explored the legal and logical boundaries of computers and network systems, IT professionals began to identify certain behaviors that benefited the institution when applied uniformly, such as the prohibition of sharing passwords or the use of “netiquette.” Then again, there is nothing like a crisis to beget an opportunity. The propagation of a computer worm by an undergraduate student at Cornell University in 1988 resulted in the creation of the oft-cited Abuse of Computers and Network Systems policy (www.cit.cornell.edu/computer/responsible-use/abuse.html) that became the foundation of many acceptable-use policies in American higher education: “Legitimate use of a computer or network system does not extend to whatever an individual is capable of doing with it.”

Such experiences informed those responsible for networks of the need for IT ethics education for the entire campus community. Policy, and the policy development process, served the dual purpose of establishing the rules and educating users. Campuses that took the lead in acceptable-use policy development generated resources for other colleges and universities. Cornell’s CPL program, for example, created a Web site that housed myriad policy-related materials, most notably the policy compendium, a library of acceptable-use policies from around the country.1 Of even greater importance, a community of IT professionals emerged who cared about and worked toward the sharing of good ideas, best practices, and communication of new developments.

IT Policy Today

In the past few years, campus IT departments have begun to develop a number of additional IT policies, covering such areas as
mass messaging, domain naming, privacy, data access and use, and security. The trend is to develop separate policies in these areas, distinct from the all-encompassing responsible- or acceptable-use policies. In addition, many campuses are looking to update those earlier broad policies in the face of rapidly changing technologies.

**Institutional Data Access and Use Policy**

Perhaps the broadest category of IT policies apart from those that deal with acceptable use encompasses policies about access to and management and use of institutional data (also referred to as electronic records). Like acceptable-use policies, these policies have a “kitchen sink” quality, bringing everything into the mix, from the library archivist’s duties, to complex enterprise resource planning (ERP) applications, to the registrar’s databases, to the IT manager’s network flow logs. Unlike acceptable-use policies, however, data use policies do not accommodate all of those responsibilities so easily.

At Cornell University, for example, data access and use policies have had mixed success. Currently, an institutional data policy makes simple statements about the responsibility of “stewards” and “custodians” with regard to institutional data, providing a comprehensive policy statement and skeleton outline of responsibilities that, like puzzle pieces, should fit together with more discrete departmental policies. A simple, clear outline of who is in charge of what data transmitted and stored on computers and network systems can go a long way toward resolving questions about access, privacy, and their attendant responsibilities. In the early 1990s, a number of universities successfully established data administration policies (for example, The Pennsylvania State University, Arizona State University, and the University of Michigan). More recently, Indiana University has developed an exemplary set of guidelines for handling electronic institutional and personal information (see [www.itpo.iu.edu/InfoGuidelines.html](http://www.itpo.iu.edu/InfoGuidelines.html)).
IT Security Policy

In these uncertain and dangerous times, there is no more important IT policy development area than security. Axiomatic from the inception of campuswide networks has been the prohibition of sharing passwords, and high-profile incidents such as the computer worm at Cornell produced some of the first statements about security in IT policy. But with the exponential rise in “malware” (electronic worms or viruses) and breach of security incidents in the past few years, not to mention the specter of terrorism since September 11, 2001, security has risen to the top of the list of IT policy concerns.

Just as there is a plurality of campus cultures, so too is there a plurality of opinion on what provisions constitute a solid security policy. Questions about network registries and authentication loom large in this context, and different campuses, according to the architecture and culture of their institutions, resolve those questions in different ways. In this sea of variety, however, IT security professionals, policy advisers, and network engineers seem to be reaching consensus on three courses of action: developing robust security policies, articulating obligations that in different degrees attach to all users of the network, and establishing designated security incidence teams, if not a comprehensive security program.

Developing Security Policies

Not surprisingly, the first recommended action is developing substantive, robust, and enforceable security policies. Given the uneven terrain of policy and policy development across campuses, this recommendation is not as simple as it sounds. It helps to have support at the highest levels of the institution. For example, in the wake of serious security breaches, Indiana University’s IT department asked for and received from the board of trustees very strong authority to correct problems with insecure and misconfigured machines on its
network that held particularly privileged data. That the board delivered these authorities to the IT shop in the form of a security policy (see www.itpo.iu.edu/ir.html) speaks to the power that policy can exercise when it is in concert with the most powerful offices and processes within an institution. The educative potential of policy, whether it comes from the top down or through a long, drawn-out process of consensus, is also invaluable.

Articulating User Obligations

Obligations that attach to users represent the substantive portion of security policies. Importantly, these obligations begin at the top of the hierarchy, with administrative heads required to do assessments of IT resources inventories and security and appoint individuals within their units to assume responsibility along these lines.

Systems and network administrators constitute a second category of users with specific duties, such as keeping abreast of security developments and deploying the most current patches, virus protection software, and perimeter protections.

Finally, all users are reminded about sharing passwords and also are put on notice that they are responsible for network security. Thus, users should not be surprised when their access is blocked under circumstances of a compromised computer on the network; rather, they should expect to do everything they can to remedy the situation in conjunction with system and network operators.

In addition to articulating the user obligations, the attention to security incidence reporting, which is sometimes included in a comprehensive security policy and sometimes separately maintained, is an important procedure to consider for policy. (For an example of a site that provides specific direction about reporting abuse, see cio.berkeley.edu/policies.html.)

Establishing a Security Team

A dedicated team of IT security professionals, headed by one person whose explicit charge is to direct security operations, coordi-
nation, and education efforts around the entire campus, is imperative at this point in the evolution of campus networking. (See Chapter Seven for additional discussion on this subject.) The security risks have become too great to manage without personnel dedicated to the task and, implicitly, the institutional support that recognizes the significance of their work.

Naming a director of security with jurisdiction over an entire campus and granting operational control to that person will represent a strong start toward setting up proper security incident reporting, virus response teams, around-the-clock bandwidth monitoring, operational password policies for servers, and authentication and authorization management.

### Mass Electronic Messaging

Mass electronic messaging policies are a subset of general statements in acceptable-use policies about the responsibility that network system operators have to regulate the system for optimal functionality. These policies identify administrative offices responsible for the permissions for mass messages, with the term *mass* usually meaning one or more of the major constituencies: faculty, staff, students, and alumni. If the institution maintains an emergency messaging program, then the policy differentiates between the emergency program and the bulk mass messaging program, usually because the emergency program will have a different effect on network performance and therefore will require different procedures.

It is increasingly common to have the university relations or college relations office involved in mass messaging policies in addition to the constituent administrative heads, because that office has a facility with official representations for the institution generally, and most certainly has a responsibility when a message is poised for dissemination to the entire community.

Given that the overall purpose of mass messaging policies is to reduce institutional spam, the bane of all users’ existence, they are usually among the least controversial of IT policies when proposed.
Nevertheless, this does not mean that struggles will not occur among administrative heads over the delegation of responsibilities among themselves. The secret in this policy process for IT personnel is to stand by and not get drawn into their contests, letting them work out the details.

Privacy Policy

If IT privacy policies are not among the most controversial, they are at least some of the most complicated. The distinction between public and private colleges and universities begins to explain why, because the relevant laws apply differently to different kinds of institutions. As extensions of the government, public institutions must take account of constitutional protections that private institutions do not have to consider. Employer–employee law as it applies to private entities with respect to electronic communications has widened that already existing public–private gap.

To date, case law recognizes full ownership and control by the employer of computer systems and their content; this body of case law offers no protection to employees. In practice, the law translates into a no-holds-barred policy on employer surveillance, including monitored transmissions, examination of stored data, and even keystroke technologies (McDonald, n.d.). Thus, while the Fourth Amendment, which covers such matters as probable cause and judicial oversight, plays a role in how a state university or college will govern the search of an employee's desk and computer, it offers no guidance to the private college or university. The law to date would appear to condone what many people would regard as arbitrary and capricious actions, such as routine monitoring for content or keystroke surveillance technologies, practices out of step with other traditions in higher education such as free speech, academic freedom, and academic integrity.

Privacy policies, in this light, take on urgency in both public and private institutions but for different reasons. Public institutions should be sure that their policy does not fall below the legal floor,
and private ones may want policy to raise the bar, if only to provide at least a modicum of dignity to themselves as employers, as well as to their employees. Just because private colleges own their networks, it does not mean that employees must work in an environment of hypersurveillance and suspicion (Cooper, 1999).

Students exist in a kind of netherworld of law and policy on privacy matters. Clearly protected in terms of whatever can be defined as an educational record under the Family Educational Rights and Privacy Act (FERPA), students nonetheless should also take a strong interest in matters of electronic privacy, if only to track the uses, and potential abuses, of their e-mail. While their mail may or may not fall under the statutory definition of an educational record, depending on its content (and developing case law), it should be more highly protected than an employee’s mail by virtue of the difference in status between a student and an employee. This is underscored by the fact that for many students, their residence hall is also their home.

Such a complicated imbroglio of issues and constituencies can surprisingly be resolved with a few simple statements and procedures. If the private institution prefers to shy away from even the mere mention of the term privacy for fear of conveying a right it intends no one to have, then it should at least establish practices that offer assurance that it will not monitor without authorization from the highest levels of administration and, therefore, it is assumed, not do so arbitrarily or capriciously. Two such practices stand out: general statements about monitoring for content and the procedures for accessing content.

The first is a statement applying to all users that it is not the practice of the institution to monitor the network for content, except in cases of reasonable suspicion of legal or policy violations. In fact, a concern that the institution either could not or would not live up to that practice has caused a minority of schools to reverse the intent and instead make it clear in policy that access is open and monitoring is the practice (Young, 2002).
The second practice is to set the authority to access material so high in the administration as to obviate concerns about competitor snooping or paranoia about network administrators reading e-mail. Those practices imply the trust that the institution places in the individuals who occupy those offices to consult the proper authorities when necessary (legal counsel, for example, or the dean of faculty) and to exercise proper judgment in all cases (Spinello, 2000).

Still newer directions in privacy statements focus on policies that concern logging and monitoring of network flow data, specifically regulations on next-step activities that resolve Internet protocol addresses into content information (Rezmierski and St. Clair, 2001). Ultimately, it is not grandstanding statements about privacy but discrete practices that give privacy policies their character (McDonald, n.d.; Mitrano, 2002; see also www.educause.edu/ir/library/pdf/pub3102.pdf and www.cit.cornell.edu/oit/policymemos/privacy.html).

**Revising Acceptable-Use Policies**

As separate policies in such areas as privacy and security are developed, what becomes of the first-generation, all-encompassing acceptable-use policies?

First, these policies can be trimmed down or bulked up depending on the point of departure. For example, if originally replete with a listing of every possible infraction, it might do well to give back to Caesar what is Caesar’s. Harassment provisions are one example. Born in the same era as sexual harassment policies, acceptable-use policies often make mention of harassment as a specific kind of violation. So long as a campus has a strong code of conduct that includes harassment, reiteration in an IT policy is probably not necessary or even appropriate.

In an age where networking has not yet seen the light at the end of the security tunnel, it is important to maintain broad statements that can play a role in the computing nightmare that we have yet to imagine. For example, the statement that “legitimate use of a
computer does not mean you may do whatever you technically can do with it" is an excellent reminder to users of ethical and policy imperatives that Internet usage or national law has yet to endorse, regardless of whether there is a separate security policy.

Finally, acceptable-use policies set the stage for other IT policies. Policy revision always presents an opportunity for education. Because the use of electronic communications will only increase with time and because it behooves colleges and universities to teach appropriate use of these resources, revisiting these foundational policies should be a permanent star in the constellation of duties for IT policy advisers and their organizations.

Conclusion

As a ubiquitous presence in higher education, IT plays an increasingly preeminent role in higher education policy development as administrators negotiate new technologies within the context of the traditional research, teaching, and service mission.

Recognizing the distinctions between the existing policies that can be brought to bear on information technologies and the areas in which there is a need for new IT-specific policy development is the first priority of any policy analyst. Ensuring that specific policies respect the institution’s traditions and personality while still getting the job done is the second. Working flexibly within the politics and policy process of the institution is the third.

The policy will be the rule; thus, there is no substitute for the careful work of understanding an institution’s design and politics, culture and traditions in the process of creating a policy. An intelligent, discriminating, and flexible sensibility should underlie all aspects of policy development.

Note

1. The Cornell Computer Policy and Law Program recently partnered with EDUCAUSE to form the EDUCAUSE/Cornell Institute for
Organizing and Managing Information Resources

Computer Policy and Law. See www.educause.edu/icpl for the policy compendium and information about the annual policy and law conference and ongoing policy officer discussion group.

References


