By Kent Wada and Paula King

IT Policy: An Essential Element of IT Infrastructure

Big pipes, cheap hardware, and clever applications provide colleges and universities unprecedented opportunities for building new services, new products, and new ways of doing business—and also expose them to unprecedented new challenges. With continuing developments in information technology (IT), the desire for academic freedom and for the open exchange of ideas and information is increasingly testing not only the operational reliability of the institutional electronic infrastructure but also the legal and ethical base of the institutional policy infrastructure. How can colleges and universities protect personal privacy in the workplace when the private sector agrees that doing so is dangerous? What is the role of an institution in regulating "cyberslacking" (surfing so much that employees don't get their jobs done)? How can institutions encourage students' academic imperatives to experiment with new technological ideas—such as Napster—when those ideas may negatively affect infrastructure? Campuses can expect to face such challenges with greater and greater frequency. How will we cope when each challenge becomes a mini-crisis?

IT Policy to the Rescue

If each challenge must be "solved" from the beginning, if there is nothing to help guide the way, if each challenge is addressed only when a high-profile, high-liability incident occurs, then there isn't much hope. The answer, of course, lies in building IT policy now, shaping process and infrastructure so that campuses have to grapple only with the unique properties of each new challenge rather than starting from scratch every time. This requires

- understanding the institution's cultural values and guiding principles well enough to be able to articulate them as institutional policy;
- identifying a core group of people who will bring needed expertise and experience to the table when grappling with a new challenge; and
- making policy a part of day-to-day practice—just another part of the IT infrastructure of the institution.

The first task—articulating an institution's cultural values—is remarkably difficult to do. But it serves as a framework that helps keep challenges manageable. Ideally, such institutional policy not only imparts rights and responsibilities but also communicates an institution's expectations and thus serves as a set of principles that can help provide answers to more operational questions on a day-to-day level. For example, how can an institution determine an appropriate level of privacy in the workplace if administrators don't understand how privacy is valued on campus? These cultural values are fundamental to the ability to make decisions that are "right" for an institution. They should infuse the entire IT policy definition and interpretation process.

Applying these principles to real-life situations is equally challenging and requires diverse experience and expertise from people who can together reason out a conclusion in a specific situation. Policy staff, technologists, and campus counsel need to work with administrators, faculty, other employees, and students in such a process. Ideally, an IT policy analyst would take the lead in building these processes and infrastructure and in ensuring that a core group is identified to quickly meet new challenges, bringing in subject experts as appropriate.

Finally, developing IT policy is a significant undertaking and needs resources dedicated to the entire process, from the definition of requirements through the application of policy to real-life cases. Institutions that do not make this policy a part of the day-to-day IT infrastructure will find it difficult to meet the challenges they will face—potentially under high pressure and media scrutiny.

A Changing Definition of IT Infrastructure

The need to add IT policy to the definition of infrastructure is in alignment with the Gartner Group's commentary in "The New Face of Infrastructure," which stated: "Most enterprises approach infrastructure from an asset-based perspective. This is a response to decentralized organizational constructs, where achieving enterprise-level synergies was subordinate to the expectation that business units succeed or fail independently, as well as to the nature of infrastructure as a collection of shared resources. Enterprises identified what asset types were shared and therefore controlled centrally, and which were not. The objective was to define infrastructure as narrowly as possible to minimize non-operating-

department intrusion of business units." The commentary describes the three most important domains as the physical infrastructure, the IT infrastructure, and the social infrastructure and notes these three domains are converging. It suggests taking a more holistic view of infrastructure: "This entails accepting a slightly more blurred but substantially more meaningful definition of infrastructure as the organization's connective tissue, a restatement that frees organizations to approach infrastructure more holistically, incorporating not only hard assets, but human, process, and organizational elements."[1]

As the definition of infrastructure has blurred, so too has the definition of IT infrastructure. Over the last decade, it has become clear that functional IT infrastructure and systems are composed of more than hardware and software. Budgeting methods that did not adequately account for the full human resources costs to analyze, design, integrate, support, and manage new hardware and software systems mostly underestimated the costs involved. If we accept a more blurred definition of IT infrastructure that incorporates not only the hard IT assets but also the human, process, and organizational elements, then IT policy development clearly deserves a greater level of attention—and on an ongoing basis.

Lessons and Actions

Several lessons may help in the formation of effective IT policy. First, technology evolves more quickly than law and business practices, and policy lags behind all of them. This isn't necessarily a bad thing, however. Good policy usually requires time to gain experience and wisdom.

Second, policy appears to require continuous interpretation, particularly given the highly mobile and transient population of higher education institutions.

Third, many real-life questions often generate a "gut-level" reaction. Ask any ten people whether Napster is "right" or "wrong," and the interesting thing is not the spectrum of answers given but how fervently most people believe in whatever answer they gave. To

overcome these natural emotional (and personal) reactions when developing IT policy, colleges and universities must use a reasoning process that involves many perspectives.

Fourth, too often IT staff are put into the awkward position of being gatekeepers, holders of the keys to some desired action (whether it be the ability to look at an employee's e-mail or the ability to send out "mass e-mail" to the entire campus community). Without a solid policy footing, suddenly the IT staff has to decide what's appropriate and what isn't, and often these decisions are made in a vacuum.

Finally, although new technology does not usually create new problems, it often sharpens an existing problem (such as copyright infringement) to the point of crisis. Many of these problems are not technology problems and are not solvable with IT policy. Instead, technologists must work with campus

policy staff to update existing policy in light of new technology. (Cyberslacking, for example, is a management problem rather than an IT issue.)

So, how can an institution of higher education develop a systematic approach to IT policy, even with limited resources? Regardless of size, the first step is to identify who needs to participate and who will be responsible for which aspects of IT policy formation, interpretation, and implementation. Many IT organizations have created an IT policy analyst position to lead the charge and to help ensure that things don't fall through the cracks. But the IT policy analyst does not create policy in a vacuum; rather, the analyst acts as coordinator and facilitator, provides analysis and project management, and serves as a bridge between the policy and the IT worlds.

An IT policy program can minimize legal exposure, deepen the campus cultural values, and in the longer run, prevent much wear and tear. There are many people and many resources that an institution can draw on to get started or to improve.[2] Use them!

Notes

1. Colleen Young, "The New Face of Infrastructure," in Gartner Group Research and Advisory Services, *Infrastructure: The Road Ahead,* September 19, 2000, <http://www4.gartner.com/Init> (accessed March 15, 2001).
2. For further information, see the following Web sites: EDUCAUSE Policy Initiatives, <http://www.educause.edu/policy/policy.html>, and the Association of College and University Policy Administrators, <http://www.inform.umd.edu/CampusInfo/Committees/Assoc/ACUPA/>.

Kent Wada is Information Technology Policy and Security Coordinator for UCLA. Paula King is Acting Director, Information Technology, for the University of California, Merced, expected to open in 2004 as the University of California's tenth campus.