

**Chapter 10**  
**The Policy Challenges**

Richard N. Katz and Rhonda I. Gross

**Web Portals and Higher Education**  
**Technologies to Make IT Personal**

Richard N. Katz and Associates

A Publication of EDUCAUSE and NACUBO

Copyright 2002 Jossey-Bass Inc.

Published by Jossey-Bass, A Wiley Company. Reprinted by permission of John Wiley & Sons, Inc. For personal use only. Not for distribution.

## The Policy Challenges

Richard N. Katz and Rhonda I. Gross

The unprecedented flow of information across networks and between organizations, coupled with the power of computer systems to extract, compile, organize, and republish information, has made e-business possible. These same capabilities are also raising significant concerns and issues related to the appropriate use of institutional information and to the protection of information originating or residing in college and university information systems.

The closing chapter of this book accurately describes the developmental phase facing colleges and universities today on the road to enabling e-business as one of *integration*. Our progress in adopting e-business in higher education will be enabled or constrained by institutions' ability to develop, implement, enforce, and automate complex rules that authorize these consumers to partake of university services. For example:

- What rights will distant learners have vis-à-vis access to licensed university information resources?
- How can colleges and universities protect usage logs that record student and faculty library consumption activity for materials licensed from third parties?

---

*Note:* The authors wish to thank Gary Gatien of the University of Michigan for his significant research in support of this writing.

- What information can and should development offices acquire and maintain on prospective donors?

The privacy, access, ownership, and security issues posed by e-business are extraordinarily complex and represent as much a set of cultural, behavioral, and policy issues as technical ones.

Colleges and universities have long—and correctly—been described as self-governing anarchies or adhocracies. Higher education's hallowed and well-established traditions of self-governance and shared governance are responsible for our remarkable history of achievement, service, and innovation. These traditions also make integration hard. In many ways, achieving the necessary level of technical integration to enable e-business is the least complex aspect of preparing the institution for e-business. Many campus chief information officers (CIOs) understand what it means to reorient systems from their current functional office views to the end user views (those of students, parents, alumni, and the inter-enterprise) that e-business will demand. In most cases, the technical tools to achieve this kind of integration exist. In short, technical integration is a significant issue that can be addressed by vision, talent, and money. The thornier integration challenges are cultural and relate to role definitions, authority and power, and values. These issues will define the boundaries of an institution's approach to, and its likelihood of success in, implementing e-business.

### **The Need for a Policy Framework to Support Portals and E-Business**

In a far-sighted article, Graves, Jenkins, and Parker (1995) describe the development of an electronic information policy framework. As e-business drives the Internet and the Web from an infrastructure for storing static information to one over which much of the institutional mission is delivered, the need for such a policy framework becomes overwhelming. Although the existence of sound informa-

tion policies will not guarantee entrée into the world of e-business, the lack of these policies will guarantee nonentrance. Colleges and universities will need to develop a cohesive and consistent set of policies that will guide the members of their communities in a number of areas, including:

- Digital identity and the access to institutional technology and information resources
- Use of the institution's name and trademarks
- Acquisition, retention, and disposition of information resources
- Ownership of information in institutional systems and the management of intellectual property rights

Each of these issues is enormously complex, and colleges and universities worldwide have struggled with them for years. No attempt will be made in this chapter to specify solutions in these areas. Rather, the purpose of this chapter is to relate the necessity of developing a holistic electronic information policy framework to efforts to implement e-business.

### **Digital Identity and Access to Institutional Technology and Information Resources**

One issue of importance is that of digital identity. In the technical context, colleges and universities must develop the means to authenticate an individual as him- or herself, to recognize the individual as a member of the institutional community, and to confer upon or deny this individual different rights and authorities as a community citizen. In physical reality, these activities are transacted in a variety of complex formal or informal ways: we can demand photo ID cards, check signature files, or wave to the familiar librarian who regulates access to the closed stacks. The regulation of

access to institutional resources in the physical context is governed by a tapestry of policies, procedures, customs, norms, and historical happenstance that computers are not yet intelligent enough to deal with. Instead, computers depend on precise information that derives absolute answers to the questions (1) Are you who you claim to be? and (2) Are you allowed to . . . (consume this service, enter this building, use this parking lot)?

Not only is this a technical challenge of enormous proportions, it is also a policy quagmire requiring colleges and universities to make explicit and public distinctions about the rights and privileges that accrue to different members of the academy. What rights does the president's spouse really have? What rights do lecturers have, relative to career-ladder faculty? These policy issues will get more complex as colleges and universities move into distance education and implement "cradle-to-endowment" strategies to create relationships with promising applicants, lifelong learners, and potential donors.

Of course, it is important to note that for public institutions, managing access to institutional information must be situated in the context of public records laws, which, themselves, are hard to reduce to simple rules that can be automated.

### **Use of the Institution's Name and Trademarks**

The Internet and the World Wide Web are, among other things, a publishing infrastructure. Web technology is relatively simple to program as well as to use, allowing "a thousand flowers to bloom." At nearly every college and university, myriad operational and dead Web pages make volumes of campus information and misinformation available to anyone with an Internet connection.

Many institutions today provide incoming students with sufficient disk storage to encourage their development of personal Web sites. Of course, into every flower garden will come the occasional weed, snail, or predator. From a policy perspective, the challenge posed by the Internet and the Web is the challenge of cultural integration. Colleges and universities must specify policies that regulate

the appropriate use of these very public resources. This is an extraordinarily complex area to govern. At stake are a variety of dire legal and public relations issues. These issues can include

- Pornographic materials on official institutional sites
- Sale of advertising on pages containing campus trademarks
- Creation of fraudulent sites
- Commercial use of campus resources for personal gain
- Trademark infringement
- E-harassment and other activities that create a hostile e-environment
- Neglect of sites that make inaccurate, anachronistic, and obsolete information available to legislators, trustees, donors, auditors, and others

All of these issues can and will emerge within the broader policy contexts that typically respect and encourage free expression by members of the institution's community. As Graves, Jenkins, and Parker advise, "any policy will need to balance the institution's role in protecting access to sensitive or potentially objectionable information and its role in supporting an individual's right of free expression" (1995, p. 18). This difficult balancing act is hardly new, but it is complicated by the levels of integration anticipated by e-business applications.

### **Acquisition, Retention, and Disposition of Information Resources**

E-business, in much of the popular literature, begins with something called "e-tailing," the marketing of the enterprise to its existing or prospective clients. In one context, for example, higher education

institutions have been doing this for years. Each year, colleges and universities acquire the files of high school students who achieve high scores on the PSAT and shower these college-bound tenth and eleventh graders with literature extolling the virtues of their campuses. In an e-business context, smart and aggressive institutions will acquire more and more information in the competition for the “best” students. These institutions will likely develop robust profiles of students to match against the target profiles of successful applicants. Similarly, the pathologies of university hospital patients will be profiled for matching against promising experimental drugs and therapies for possible “targeting” of such patients for clinical trials.

These practices are entrepreneurial, effective (relative to their goals), and probably beneficial, as college-bound students “want” to be discovered and patients want access to the best modes of treatment available. However, the unprecedented ability of institutions to acquire personal information, to combine this information in unique ways, and to store massive amounts of this information on individuals who may (or may not) be part of the institutional community, will raise significant privacy and security issues in the future. New policies regarding what kind of information is to be collected, how it is to be used, and for how long it is to be retained, will become increasingly important. The failure to develop new standards of practice in this area will invite new regulation of this area of institutional activity. The issue of individual and institutional access to this kind of information will also rise in importance and must be dealt with explicitly in campus information policy.

In addition to developing the technologies and policies to ensure privacy and to secure and protect information under institutional management, colleges and universities will need to devise and implement new policies to describe, manage, and protect related classes of information. Such classes of information include confidential information (tenure and promotion files), proprietary information (patent, trademarks, copyrights), privileged information (attorney-

client communications, counseling files), and trade information (public-private research activities). E-business, among other things, assumes an unprecedented level of interoperation among the systems and data resources of “trading partners.” In the future, campus suppliers will have access to institutional procurement systems, as will publishers, high schools, consortium partners, and others. This integration of systems and information will demand that policies and contracts regulate the acquisition, use, retention, and disposition of information by others in the newly extending community. This has already become a very complex area of policy development at research universities where the university values of open sharing of research findings clashes with desires of private clinical research sponsors to protect information as proprietary.

A final area of concern under this broad umbrella is the management of licensed software and information resources. Campus information policy must respect the rights of authors and distributors. Evolving technologies and law will likely enhance authors’ and distributors’ ability to track the use of their licensed property and perhaps even to implement campuswide penalties when infringements are identified.

### **Ownership of Information and Intellectual Property Rights**

Information policy must seek to distinguish the ownership status of information embodied in institutionally owned digital storage and transport media from the responsibilities for managing this information. Information policies should strive to define the standards and care with which information resources must be managed, while recognizing the inherently decentralizing tendencies of networked information and resources. Most information policy frameworks that address networked information define and articulate a concept of information stewardship that allows the Web of campus-related information to evolve in a fashion that balances the needs of individuals and local campus units with those of the institution as a whole.

Perhaps the most complex aspect of preparing the campus information policy environment for e-business is the set of policy issues surrounding the ownership and management of intellectual property generated on the campus. Whereas colleges and universities have developed robust policies for the ownership and management of intellectual property protected by patents, the rights to intellectual property developed by faculty members and protected by copyright have traditionally remained with individual faculty members. To be frank, the total economic value of published college and university intellectual property has been small historically, and the institutional investment in the creation of this property has also been small.

The application of Internet, Web, and other information technologies to the core educational mission of higher education is changing all of this. Today, pioneering faculty members are investing considerable time and energy to Web-enable their courses. Institutions, in many cases, are partnering with these faculty members by providing grants to purchase release time from other obligations and by placing a variety of technical tools at the faculty member's disposal. For the first time, course materials organized in this fashion can reach beyond the confines of the classroom, hence changing simultaneously the cost structure, the investment model, and the economic value of traditional course materials. Courses created in this fashion become courseware and begin to accrue many of the attributes of books, which also are evolving to become more interactive.

As the e-learning aspect of the e-business revolution evolves, institutions, their faculty members, and publishers are looking at faculty course materials as scalable economic goods that can be modularized. New pedagogical standards are evolving, in concert with new neuroscientific findings about the learning process. Institutions such as the University of Phoenix and Great Britain's Open University are investing millions in curricula for networked delivery. Faculty course notes on the Web are being reportedly pirated and repackaged for distribution by new proprietary e-business enterprises. In sum, the new potential posed by the integrated technolo-

gies of e-business suggest the need for new policies regarding the ownership and management of rights to faculty course materials.

Framed creatively, this discussion and faculty and institutional investments can draw new students into the campus community and, in some cases, bring new revenue to the institution. Such changes are, however, countercultural and could also lead to new divisions on the campus. As noted in Chapter Six, e-business is likely to change the way institutions operate. It is a mission-critical undertaking that will challenge long-standing institutional policies and will therefore demand the careful application of change management techniques and processes.

## **Elements of an Integrated Policy Framework**

Although each institution will develop a policy that best reflects its priorities, strategies, values, and history, a policy framework should contain certain elements. The list that follows is offered as a starting point to encourage the reader to begin.

### **Critical Assumptions**

The institution will balance the rights of individuals with the institution's responsibility to make information available to support the mission. The role of the central campus is to articulate the standards of data access and integrity and to differentiate user rights and privileges so as to achieve such a balance. A key question that will need to be considered is, under what conditions (responsibilities of resource users) and for what members of the community are access to the network, network-based services, and networked information a basic right of the campus community?

### **Operating Principles**

Policies are, by definition, value-laden. Institutions can be well served by considering bounding the framework by principles. At many institutions (particularly public), information policy is bounded by principles that

- Identify the responsibility for making information available
- Limit the institution's regulatory responsibility for information for which it is not responsible
- Assume institutional responsibility for defining access privileges to its information for classes of users

Such a policy framework and those of other leading institutions also outline in broad terms a variety of legal, ethical, technical, governance, and economic issues for the purpose of acculturating the policy reader to the complexity of the issues and to the basic values of the institution.

### **Information Access and Security**

It will be important to establish the notion that institutional electronic information resources—including data, applications, systems, hardware, software, and networks—are valuable. Institutional assets, including electronic information resources, must be protected according to the nature of the risk and to the sensitivity and criticality of the resource being protected. Information policy should endeavor to identify major classes of information assets requiring protection and assign to them differential levels of protection. Information classes might include privileged information, personal information, personnel information, public records, and so forth.

Areas in which security-related policies need to be addressed include the following, drawn from the University of California's *Business and Finance Bulletin IS-3* (Nov. 1998):

- *Logical security.* The policy should identify security measures to be enforced through software, network, or procedural controls (such as version management) as well as communications security and reduction of risk from intrusive computer software. Various measures

include end-user access controls, system administration access controls, applications software development and change control, and controls on data backup, retention, data privacy, and data transfers and downloads. Encryption policies will also need to be developed, as these capabilities become ubiquitous, as will policies that specify which applications and resources must be protected by firewalls.

- *Physical security.* Even in an e-business environment, there are physical disaster controls and access controls (for example, for check stock and other financial instruments) that must be covered by institutional policy.
- *Managerial security.* Although there are unique risks inherent in the management of electronic and, particularly, networked information resources, many of the risks remain people-related. An information policy framework should attempt to integrate institutional policy related to bonding and background checking for personnel with access to sensitive and critical information. Procedures to implement such policies should also identify the processes for altering authorities when changes in duties or employment status occur.
- *Responsibilities.* An information policy framework must identify both those responsible for maintaining the policy and those responsible for its implementation. Ideally, policy compliance escalation procedures should be specified.
- *Definitions and authorities.* A policy framework should define key terms such as *authorized user*, *disaster*, *security*, *virus*, and others. Information management roles such as stewardship and proprietorship should also be defined. Regulations and laws that govern an

institution's access and security policies should be referenced, including public records law.

- *Digital certificates.* An emerging technology to meet the needs of electronic security in the networked context is the use of public key infrastructure and digital certificates. This technology is being developed to address authorization and authentication. Institutions that implement certificate authorities and digital certificates will need also to develop congruent policies that identify processes for approving authorities, standards for certificates, and identification of certificates. Policies will also have to be enacted to govern whether certificates are issued to individuals, servers, or certificate authorities, what the responsibilities of these authorities are, and what the expiry dates of these certificates will be. Finally, policy in this evolving arena will need to describe the processes for registering and issuing certificates, for maintaining a repository of certificates and public keys, for revoking or renewing certificates, and for managing the certificate authority's private key.

### **Disaster Protection and Business Continuity**

Institutions must also develop policy environments that protect their information resources systems and services.

- The information policy framework should describe the institution's plans, policies, and procedures for assuring business continuity, including plans for testing critical systems periodically.
- The disaster recovery plan should identify emergency response procedures, and it should specify teams of per-

sonnel responsible for responding to emergency situations.

### **E-mail**

Although e-mail is not specifically a tool of e-business, its governance as a critical element of the overall campus information policy framework is crucial. Institutions are advised to develop specific policies related to electronic mail that establish the following:

- E-mail accounts as institutional property
- The institution's service commitments regarding e-mail
- The ownership of information produced and received using e-mail accounts
- Institutional access to information in mail accounts under normal or extraordinary (emergency or investigative) conditions
- Allowable use, including use for individual commercial gain, representations, and false identity
- Security and confidentiality of information in e-mail accounts
- Individual and institutional responsibilities and authorities for ensuring compliance with policy

### **Intellectual Property**

Policy related to the management and ownership of intellectual property is most complex. For intellectual property not developed on campus and covered by copyrights, patents, licenses, or other contracts, the policy parameters tend to be straightforward.

- Software residing on institutional hardware must be used according to the terms specified under the appropriate software license agreement.
- The institution is responsible for compliance with licenses entered into by the institution on behalf of members of its community. The institution should maintain the right to revoke licensed privileges in cases where violations have been identified. Substantial violations of license conditions should be specified under policy, as should the process for investigating alleged misuse and for implementing remedial action.
- Information resources, such as databases, books, journal articles, and the like, are governed by either copyright law or license agreements with their publishers. Institutional policy should affirm the rights of authors, publishers, and distributors to their intellectual property, it should define what constitutes “fair use” in the context of law and licenses, and it should identify the processes for investigating alleged misuse and for implementing remedial action.
- For intellectual property developed on campus, the institution must distinguish between so-called works-for-hire and other works produced in the discharge of an employee’s work-related role(s).
- The ownership of a work-for-hire is generally assumed to be the property of the institution. The information policy framework should make explicit reference to the institution’s assumptions about what works are considered to be works-for-hire and what ownership rights the institution wishes to assert. This policy should also specify what rights individuals creating works-for-hire may have (publication of a work report in a profes-

sional journal), and what the process is for securing individual access to such works.

- The rules of policies related to ownership of other intellectual property produced by members of the campus community are more likely to be specified in an institution's faculty handbook, or in policy covering patents, or even in policy covering conflict of interest and commitment (Thompson, 1999). As the boundaries between course materials and published materials begin to blur, institutions will need to revisit the ownership issues as part of an integrated information policy framework.

Policy is, by its nature, soft, squishy, and difficult. As previously mentioned, policy development and the policy environment are inherently value-laden, and therefore there are no cookbooks or detailed instructions for their formulation. Policies are for the most part context-specific. A bible college's definition of appropriate use of technology will likely differ from that of a public research university.

Policy can be integrative, and integration is the mandate that looms ahead for institutions seeking to implement e-business solutions. Colleges and universities anticipating the move to e-business must recall that e-business, in many areas, is not merely the application of new technology to old processes. E-business applications will open new vistas and create new risks. Extending the name and reach of your college or university can and will swell the ranks of members of your communities. As e-communities grow, opportunities grow. Along with opportunities, fraud, abuse, and misuse will also grow. An integrated information policy framework will be hard to institute. On the other hand, an integrated, e-business environment without a supporting policy framework will be nearly impossible to manage.

## References

- Graves, W., Jenkins, C., and Parker, A. "Development of an Electronic Information Policy Framework." *CAUSE/EFFECT*, Summer 1995, pp. 15–23. [<http://www.educause.edu/ir/library/pdf/cem9524.pdf>].
- Thompson, D. "Intellectual Property Meets Information Technology." *Educom Review*, 1999, 34(2), 14–21. [<http://www.educause.edu/ir/library/html/erm99022.html>].
- University of California. *Business and Finance Bulletin IS-3: Electronic Information Security*, Nov. 1998. [<http://www.ucop.edu/ucophome/policies/bfb/is3.pdf>].