

Web Site Privacy Policies

The reminder arrives in your inbox: “Time to review Web site privacy policy.” You ignore it for a few weeks, but eventually you rediscover it during a spirited spring-cleaning of your inbox. You finally set aside some time to work on this project, but now you’re stumped. Where do you begin? Why do you need a privacy policy? What elements create such a policy? What are peers doing about their Web site privacy policies?

The first issue to be addressed is the concept of *privacy*. Privacy involves (1) the basic right to not be bothered (*anonymity*), (2) the right to control how, when, and what information is revealed about oneself (*confidentiality*), and (3) the belief that entities collecting private information will take measures to protect that information (*security*). In higher education, privacy is seen as a critical ingredient for intellectual development and freedom.¹ Colleges and universities are in a unique position: they must balance an individual’s right to privacy with the public’s rights to know. A Web site privacy policy thus outlines the institution’s role and its information-gathering practices and engenders trust with its community of users.

Classic Privacy Policies

Classic privacy policies are short and simple and are divided into three sections: information gathering; information use; and cookies. The first section of a classic privacy policy defines the information that the Web site gathers from users. This usually includes a user’s IP address, Web pages the user has visited (location, date, and time), referral Web pages that delivered the user to the gate-

way site, and the user’s browser and operating system information. Sometimes this section will include language clarifying the personally identifiable information that is *not* collected. In the second section, the information use section, classic Web site privacy policies outline how the gathered information will and will not be used. Users are told that the educational institution will not provide or sell the collected information to third parties, such as those outside the educational institution, unless mandated by law. The privacy policy usually states that the collected information is used to improve Web site usability and that aggregate information is compiled to solve performance-related questions. Sometimes policies will state that IP addresses will not be combined with site-usage data. Third, the cookies section of the classic privacy policy describes the use of these tiny text files to recognize a user, customize parts of the Web site, and measure gateway traffic. The privacy policy may declare that cookies do not gather user demographic data. Contact details—usually the name of the Web site administrator and a disclaimer—wrap up the classic privacy policy.

Next-Generation Privacy Policies

State rules, regulations, and laws created in the past few years have forced educational institutions to upgrade their information technology policies. Thus, next-generation privacy policies are more detailed and longer, and they reference state laws. The information-gathering, information use, and cookies sections are more detailed and are joined by newer elements such as sections on information

disclosure, retention, procedures for access and review, and confidentiality/integrity.

In next-generation privacy policies, the information-gathering section has been expanded to explain technical pieces of Web site interactions. The University at Buffalo’s Web site privacy policy, for example, identifies and describes twelve pieces, including the content length in bytes, the Universal Resource Identifier (URI), the query string of the URI, and the transport protocol (<http://www.itpolicies.buffalo.edu/privacy/>). The Web site privacy policy at the University of Minnesota adds search terms used in the Web site’s search engine. Minnesota’s policy also explains the use of monitoring software that logs e-mail headers and network packet addresses for the purposes of securing its network (<http://www.privacy.umn.edu>). This is an important addition given the fact that institutions are spending more resources authenticating users, identifying illegal network activities, and removing virus-infected resources for quarantine. The cookies section in next-generation privacy policies describes the difference between session and persistent cookies and explains the various cookie settings that users can configure in their browsers.

An additional element in the next-generation privacy policies is the information disclosure section, which explains the types of information that consenting users may voluntarily provide the educational institution when using its Web site. Users who complete a transaction, fill out a survey, request information such as a catalog, e-mail staff using a Web form, or sign up for a listserv are exam-

ples included here. These users usually provide personally identifiable information, and the educational institution pledges to use it responsibly to complete a user's request. Again, users are reminded that this information will not be shared or sold to parties outside of the educational institution unless the institution is complying with law enforcement authorities. The Family Educational Rights and Privacy Act (FERPA), the USA-PATRIOT Act, and state open-records laws are referenced in the disclosure section as well.

Other elements of next-generation privacy policies include sections on retention, procedures for information access and review, and confidentiality/integrity. Electronic records and access logs created by Web sites are retained, maintained, and disposed of based on a retention schedule. Time periods are defined for keeping these records on servers, archiving them onto stable media such as CDs, and destroying the records. Procedures for information access and review spell out the rules for a user to request any personal information that has been collected. Usually a privacy compliance representative is named, and a time period to respond to user requests is given. This section also defines reasonable proof to verify user identity. Finally, the confidentiality/integrity section names who should handle the information collected and how it should be handled. Limiting access to the collected information and using authentication and encryption are specific steps identified here.

Web site privacy policies are not just for gateway dot-edu Web sites. Tailoring basic privacy policy elements to sites devoted to course management systems, human resources systems, health systems, and academic departments can be important. In course management systems, defining which information is public (e.g., discussion boards) and not public (e.g., grades and private communications) and tracking or monitoring procedures can set appropriate user expectations. Privacy concerns about personally identifiable information increase when using Web-based human resources systems. Since many benefits tasks are now completed online, creating privacy policies

that include integrity and confidentiality elements increases users' trust in these systems. Health systems Web sites usually include a general privacy policy and a detailed notice of privacy practices relating to the Health Insurance Portability and Accountability Act (HIPAA). Lastly, departmental Web sites can customize institution-level policies to match their needs. For example, a department may decide to retain information collected from Web sites indefinitely for future analysis.

As laws and regulations slowly catch up with information technology, policies are increasingly being developed in areas such as general use, acceptable use, copyright, and intellectual property. Privacy policy elements can be found in some of these other IT policies, but a privacy policy link directly on a Web site helps users understand how their privacy is treated with regard to network security and applicable laws. The University of Minnesota even has a policy regarding Web site privacy policies. Two faculty members assisted in writing the policy, which helps campus units to determine if a Web site privacy policy is needed and, if so, to create one. The academic policy (http://www.fpd.finop.umn.edu/groups/ppd/documents/policy/Online_Privacy.cfm) includes sections for definitions, staff responsibilities, reasons for the policy, a FAQ (Frequently Asked Questions) list, and customizable policy examples.

Public Policy Implications

Student financial information highlights some of the issues surrounding the public policy implications of privacy practices and policies. Since May 23, 2003, the Gramm-Leach-Bliley (GLB) Act has mandated privacy protection and the defense of customer financial information. College and university financial aid activities, such as administering federal student loan programs, fall under the act. Institutions protecting educational records in order to comply with FERPA also fulfill GLB privacy compliance but must meet additional requirements related to the safeguarding of student financial data.² These requirements include developing an information security management program and providing privacy notices to customers. In December 2003, the Fed-

eral Trade Commission and other agencies requested public comments on how to improve privacy notices so that customers can better understand how their financial information is handled.³ Specifically, the agencies were looking for input on a model privacy notice that would be short and simple. Although the agencies have not yet reached a decision on model privacy notices, others are considering alternatives to current policy practices. Responding to recently approved European Union data-privacy initiatives, commercial Web sites are starting to develop shorter, modular privacy notices linked to longer policies.⁴ Educational institutions outline some of their privacy practices in FAQ lists and in training manuals for financial information staff, but surveys continue to show the importance of clear, concise privacy notices. Although not mandated to satisfy the GLB Act or FERPA, posting such notices on financial Web sites improves transparency and represents good information management practices.



Web site privacy policies will vary based on institutional size and culture, but future federal and state laws and the increasing desire for conciseness will create more opportunities to update campus guidelines. The reminder in your inbox cannot be ignored: you must review your Web site privacy policy. Doing so reflects the institutional mission of balancing the privacy of individuals and the confidentiality of data with network integrity efforts and public safety needs.

Notes

1. *Privacy and the Handling of Student Information in the Electronic Networked Environments of Colleges and Universities* (Boulder: CAUSE, 1997), p. 4, <<http://www.educause.edu/ir/library/pdf/PUB3102.pdf>>.
2. "Colleges and Universities Subject to New FTC Rules Safeguarding Customer Information," *NACUBO Advisory Report 2003-01*, January 13, 2003.
3. Proposed Rules, "Interagency Proposal to Consider Alternative Forms of Privacy Notices under the Gramm-Leach-Bliley Act," *Federal Register*, vol. 68, no. 249 (December 30, 2003): 75166.
4. Jaikumar Vijayan, "Companies Simplify Data Privacy Notices," *Computerworld*, January 10, 2005, <<http://www.computerworld.com/databasetopics/data/story/0,10801,98812,00.html>>.

Vishant Shah recently completed an internship with the EDUCAUSE policy team in Washington, D.C.