Development of an Electronic Information Policy Framework

by William H. Graves, Carol G. Jenkins, and Anne S. Parker

The University of North Carolina at Chapel Hill, like many other universities, is attempting to manage an unprecedented demand for electronic information in myriad forms. Issues of availability, responsibility, confidentiality, privacy, and security are not easily resolved when accountabilities intersect across non-intersecting central organizations. This article summarizes the strategies and rationales employed in creating a coordinating council to develop a policy framework articulating the electronic rights and responsibilities of the university community and the public, and includes a copy of the current policy.

The purpose of this article is to report the evolution and current status of the policy framework for electronic rights and responsibilities at the University of North Carolina at Chapel Hill (UNC–CH). The framework was developed by a partnership of information technology, library, and administrative leadership at the University. This description of the framework and the processes that shaped and continue to guide its implementation may prove useful to others who recognize new, technological windows on old issues in the following scenarios:

➤ A teenager dials into a machine at a university in his city. From that connection, he establishes a connection to another machine at a distant university. This machine allows him to establish an Internet connection and thereby a connection to alt.sex. His father and the press in his city express outrage that the two universities separated by miles have conspired electronically to lead America’s youth astray.

➤ The FBI, suspecting that a nefarious hacker has broken into a machine in the physics department at a college, demands a copy of that machine’s fixed disk from the department chair. The chair seeks legal counsel and is advised to comply with the FBI’s demand. The FBI now has a copy of many files considered private by their creators in the department.

“The overall goal is to make the information needed by the University’s various constituencies as accessible and useful as possible.”

Bill Graves, as Associate Provost for Information Technology at UNC–CH, chairs the University’s Information Resources Coordinating Council and, on the national front, chairs the planning committee for Educom’s National Learning Infrastructure Initiative. He is also Director of the Institute for Academic Technology, Professor of Information and Library Science, and Professor of Mathematics at UNC–CH.

Carol Jenkins has been the Director of the UNC–CH Health Sciences Library since 1986. She has held similar positions at the Oregon Health Sciences University, University of Virginia Medical Center, and University of Maryland at Baltimore. She serves on the UNC–CH Advisory Committee for Information Technology and the Information Resources Coordinating Council.

Anne Parker has twenty-seven years of varied experience in information technology, with over nineteen years of providing research and instructional support at UNC–CH. For the past three years, she has been OIT’s deputy director, and also represents OIT on many committees including the Information Resources Coordinating Council.
A state auditor advises a university chancellor that the university should have a special university policy to guide the personal use of university-owned computers and related electronic property, including e-mail. The tenor of the advice is (1) that all personal use should be prohibited, even if it adds no incremental cost and possibly contributes to professional development and an environment of open expression, and (2) that digital technologies demand special personal-use policies different from those formulated for other university-owned property.

An administrator finds herself having to respond to requests for large amounts of data from administrative files, for public use, in the format requested. How can she cost-effectively respond to such requests, mandated by law, while doing her best to provide data that accurately describe the college, are not misleading, and protect individual privacy?

Libraries and other campus agencies have leased network access to commercial databases. How can licenses for access to such databases reflect the broadest access possible to meet information needs of campus users, avoid costly duplication, and be enforced and supported through user support services?

University administrators from units all over campus search for information to support reaccreditation and find that institutional data were not readily available when the need arose.

Individual departments and schools at a university create World Wide Web home pages because the technology is available. Little, if any, consideration is given to the quality of the information, how it will be maintained, or what standards should be incorporated.

Each of the above scenarios is based on an event that informed or continues to inform UNC-CH’s work on the policy framework. In fact, new examples supporting the need for a coordinated institutional approach to information policy arise almost daily.

An overview of UNC-CH’s policy framework

The policy framework developed at UNC-CH is appended to this article in its present form as Appendix A. It describes the nature of the University’s network and proposes a set of overarching University-wide rights and responsibilities for both consumers and producers of networked information. The overall goal is to make the information needed by the University’s various constituencies as accessible and useful as possible. The document is only a policy framework, a statement of philosophy, but it should be read with the understanding that unit-level producers/providers of information resources will be required to develop policies and practices consistent with the new University-wide framework. Indeed, the framework document proposes several new directions that depart from current practice at UNC-CH:

(1) The University will have ultimate responsibility for all official, institutional information generated at unit levels. Current policy, in contrast, places this responsibility solely at the unit level. The University will expect units to act as responsible stewards of the information that they generate. Stewardship will include the responsibility to prepare and manage information in compliance with University-wide standards and practices.

(2) The University will expect the units to “publish” institutional information in a comprehensive manner on the University network with enough searching, browsing, and “mining” capabilities to provide aggregate information about the people and other resources of the unit. Such information includes, for example, information about students, faculty members, unit expenditures, and other fiscal activities. Many units will choose to use electronic publication to provide information about the content and direction of their academic programs and activities, but academic work remains the private property of individual scholars, students, and staff members except as dictated by external funding agencies, state and federal policies, or various contractual arrangements. The intent is to “open” official, institutional information at the unit level to all members of the University community and to anyone who has Internet access from anywhere. Current practice, in contrast, exhibits much less openness. The formats of the electronic presentation of information will be carefully designed to be broadly useful, permitting the University, within the scope of the law, to reject requests for information in other formats that are not easy to accommodate.

(3) Information embodied in University-owned digital storage and transport media will be considered private property except when specifically intended to be an official University communication or record or when otherwise treated by a contractual arrangement or federal or state laws. This includes non-official electronic mail, which presently is not consistently viewed as private.

The first two directions are an attempt to open the University’s “official” institutional
records to a broader audience, especially within the University. Open access to information is increasingly important to the University’s competitive position at a time when intellectual capital is encroaching on physical capital as the driving force in the world economy and order. Indeed, openness is becoming the expectation in North Carolina, as this recent statement from Governor Hunt suggests: “Members of the public and the media need to have access to this computerized information about their state government, and we should make those records as accessible as possible.” In contrast, the third direction is an attempt to put a “privacy” stake in the ground in an area where the law is unclear and is often uninformed on the nature of the digital revolution.

Nor is the University immune to the pressures forcing all institutions—public, non-profit, and commercial—to become more accountable and cost-effective. Academic governance for years has modeled the “flat” structures touted today by the corporate world as essential to competitiveness. But the effectiveness of the flat model is dependent on the open flow of information. Now for the first time, paper-moving impediments to openness can be mitigated by capturing, storing, and sharing information across digital networks. The new technologies can advance educational quality in a timely, cost-effective manner by improving collegial decision-making with the support of nimble administrative and business processes and an open information policy that addresses key issues.

**Issues to be considered in an institutional information policy**

An information policy should acknowledge that there are complex legal, ethical, technical, governance, and economic issues that need to be addressed. Defining these issues does not necessarily mean that the way to deal with them is clear. Networked access to electronic information is still a new phenomenon to many users and institutions; thus an institutional policy should provide some guidance, but be flexible enough to allow the lessons of experience to mold practice. Some basic assumptions and operating principles set the stage for defining the institution’s role at UNC–CH. These may ultimately be incorporated into official policy, if they are supported by the University community. With these assumptions and operating principles in mind, a committee defined issues in three key areas: legal/ethical, technical, and governance/economic. We abstract these basic assumptions, operating principles, legal/ethical issues, technical issues, and governance/economic issues below.

**Basic assumptions**

Four basic assumptions provide the foundation for defining key policy issues:

- It should be possible to provide timely access from a desktop workstation to needed information, regardless of its location and format, for members of an institution’s community. This assumes the availability of a network infrastructure, including distributed computing resources and communications, and also assumes external and internal compatibility.
- It should be possible to find a balance between the rights of individuals, as authors and as users of information, and the responsibilities of the institution to make information available to support scholarship, instruction, and service. This is a fundamental balance between privacy and access.
- It should be possible to define different classes of users of institutional information, each with different access privileges, and to regulate such access accordingly.

**Operating principles**

Three operating principles define how the institution will behave in fulfilling its policy obligations:

- The institution will define the information that it is responsible for making available electronically, putting itself in the role of electronic publisher/distributor. This will require (a) a robust network infrastructure and a policy governing access to it, and (b) publication of the information on the network.
- The institution will not regulate access to networked information for which it is not responsible. This will be the responsibility of authors and readers. However, the University will support unregulated access to networked information under conditions specified by its authors.
- The institution will define access privileges to its information for classes of users.

**Legal and ethical issues**

The key legal and ethical issues revolve around concerns for protecting an individual’s right to privacy and the rights of authors and distributors. Any policy must address individuals’ privacy and identify classes of information protected by law and federal regulation. Policy must recognize, for example, protection currently in place in federal grants involving human research subjects.

Policy must also be sensitive to the needs of
the community of both knowledge creators and users, protecting the legal rights of authors/distributors, protecting contractual agreements in software licenses, and facilitating and complying with archival requirements. Many of these issues currently are being debated nationally in an attempt to find a common ground for ensuring that information in electronic form can be made readily available to support scholarship and discovery in a manner that protects the ownership rights of authors and distributors while taking advantage of opportunities for improved access via networks.

Policy must respect the basic rights of authors and distributors and the confidentiality of sensitive information. This raises both ethical and legal issues. Authors and distributors have the basic right to acknowledgment and the right to determine the form, manner, and terms of publication and distribution of their work. An institutional information policy should provide mechanisms for safeguarding these basic rights. Further, 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. These are some of the most difficult issues to tackle in any environment that at present allows highly unregulated access to academic information, while tightly controlling access to most administrative information.

Technical issues
Institutional information policy should support the adoption of technical standards and practices that ensure appropriate accessibility and security of data and appropriate data integrity. Policy must ensure that data are reachable in a usable format by authorized users. Standards for connectivity will address access to data through both direct (e.g., ftp) and indirect methods (e.g., “sneakernet”). Standards for authorization will suggest methods for authentication and encryption of data to protect its accessibility by eligible users. Standard data formats should be recommended to ensure the widest possible readership. To assure quality control and data integrity, policy must ensure that data are stored, backed up, and transmitted according to standards and protocols that preserve data integrity. Standards and responsibility for archiving and accurately transmitting institutional data should be guaranteed.

Governance and economic issues
If an institutional information policy defines the institution’s role as publisher/distributor of certain kinds of information about the institution, then it also should identify which units are responsible for guaranteeing access to that information. Some of the key questions about governance include:

• Which officer or group is responsible for ensuring appropriate access to institutional information? This role incorporates the legal, ethical, and technical responsibilities outlined above to promote appropriate access to, and availability of, institutional information. It also includes educational and consultative responsibilities to promote the appropriate use of institutional information. In addition, it includes fiduciary responsibility for providing and maintaining information resources. UNC–CH’s information policy framework suggests that schools and departments that are responsible for the content of information can also be responsible for all of these aspects of access to that information, given a strong policy and a robust, pervasive infrastructure.

• What is the institution’s responsibility for access to non-institutional information? UNC–CH’s policy framework suggests that, beyond the University’s obligation to provide Internet service to faculty, staff, and students, this responsibility rests with the author or reader, not with the University.

• Which officer or group determines the rights and privileges of different classes of users? This question also raises the issue of whether access to electronic information should be free or fee-based.

Developing a policy framework
In 1992, the University’s Advisory Committee for Information Technology (ACIT), responding to events such as those described in the opening scenarios, appointed a subcommittee to outline key issues and considerations that a University-wide information policy could help address. (The University’s two chief academic officers—for Academic Affairs and Health Affairs—created the faculty-based ACIT to advise the associate provost responsible for the University-wide network and the University’s central investments in academic computing and classroom technologies.) The subcommittee drew upon campus expertise as well as the experiences of other universities in defining the assumptions, principles, and issues described in the preceding section. (A list of references used by the committee and subsequent groups working on the policy framework is included at the end of this article.) During the subcommittee’s deliberations, the two academic officers and the University’s chief financial officer created the Information
Resources Coordinating Council (IRCC) to coordinate the management of pan-University digital information stores and technologies distributed across organizational boundaries that intersect only at the level of chancellor. The Council includes library leadership, academic and administrative information technology leadership, and the chair of ACIT. ACIT then decided that the work of its subcommittee on information policy was more appropriately the domain of IRCC.

After reviewing the key issues and guiding principles articulated by the ACIT subcommittee, IRCC decided that the development of information policy or policies would be a long-term process that would benefit from a policy “framework” document. IRCC proceeded to develop a framework document and then “proofed” the document by applying test cases to its key concepts. The test cases derived from a discussion of the current electronic mail environment, a meeting with the University Registrar to discuss the framework’s compatibility with current practice and planned direction for student information, and a meeting with representatives of a grass roots staff initiative aimed at coordinating and developing standards for document imaging initiatives. The policy framework was demonstrated to be highly compatible with the desired directions in the areas tested. Thus far, the only omission exposed by case testing is a lack of archiving considerations. Some current practices for electronic mail, however, contrast in minor ways with the philosophy stated in the document and are being revised accordingly.

The resulting version of the framework was then presented to a group of University vice chancellors—those responsible for University academic, research, and business matters. The vice chancellors voiced strong concern about protecting the privacy of academic research conducted over electronic networks. They agreed that using the term “institutional information” would help clarify how the University wishes to distinguish between public and private information. They recognized that many difficult issues would surface again during implementation of the framework and the evolution of a governance structure to resolve disputes. The meeting ended with an agreement to obtain feedback on the policy framework from deans, faculty, administrative officials, and perhaps the grass roots staff-based Employee Forum.

Garnering support and gathering feedback
IRCC has sponsored presentation/discussion meetings with several important constituencies: a group of ten faculty members, the deans in Health Affairs, the deans in Academic Affairs, the Executive Committee of the Faculty Council, the Faculty Council, the Division of Business and Finance, and the Chancellor’s Administrative Council. With the exception of the session with the Faculty Council, these meetings were conducted as small focus-group sessions framed by a presentation. Well in advance of each meeting, each participant received a copy of the draft policy framework and a letter describing what was to happen at the meeting and why the policy framework was important. A few days before the meeting, invited participants received a list of potential benefits and a list of questions to consider for the discussion.

With the exception of the Executive Committee of the Faculty Council, each group had difficulty separating the policy framework from the issues that will have to be resolved during implementation. Concerns common to all groups fall within three primary areas: (1) financial support, training support, and other infrastructure support for implementation of the framework; (2) definition of “institutional” information; and (3) privacy.

Given the budget constraints of the University, some faculty questioned whether the expectations raised by the policy framework were realistic, while others, noting the growing amount of institutional data already online, wondered about the need for such a policy. Many faculty wondered if they would be able to utilize online resources without time, incentives, and support from department chairs and deans to familiarize themselves with new technologies.

Many participants from each group asked for a specific definition of “institutional information”—an example of participants’ difficulty in differentiating conceptual framework from implementation. In response, IRCC members reiterated their hesitation to determine what should and should not be “published” online without input from departments during the implementation process.

Deans echoed these concerns and also suggested that the central administration adopt a pan-University “vision” of the use of electronic information. They were very receptive to the idea of the Internet as a marketing tool for their programs, but some worried that making more information available would increase individual workloads through requests for more details or requests for services. The deans clearly wish to be involved in determining the scope and nature of institutional information and want a high-level commitment to addressing the cost issues. They agreed that this is not solely a technology issue.

Privacy and appropriate use issues arose but not as a pressing issue for most faculty members.
Most agreed that a proactive stance on these issues would help guide the University’s decisions on policies in the future and would place the University in a stronger position in case of a legal entanglement over these issues. There was, however, strong agreement among the deans that faculty and other University employees need to be made aware of the unique qualities of electronic mail as a means to create, send, and store information. The deans expressed concern that many people still look at e-mail as a secure and highly protected medium.

The presentation/discussion meetings revealed that people have a hard time “getting into” a discussion about something that is abstract and outside their experiences. The scenarios presented in advance of the meetings were beneficial, but more was needed. Additional stage setting might have helped people understand why information policies are important. Futuristic scenarios might have been helpful if balanced against today’s scenarios. What would it be like if the policy framework were in place?

Providing participants with a brief summary of the follow-on implementation issues (legal, ethical, technical, governance) also might have helped focus discussion on the framework itself rather than on implementation. Participants focused almost exclusively on departments as providers of information, rather than as consumers. It might have been valuable to inquire specifically about departments’ information needs.

Nevertheless, reviewers generally accepted the policy framework and agreed on the need for, and utility of, a set of defining principles to guide development of future policies and practices. They also recognized that early involvement of the highest levels of the administration would encourage more sound and consistent policy decisions in the future. Toward this end, IRCC recently asked the Chancellor’s Administrative Council to endorse that policy framework, and the Council did so.

Implementing the policy framework

With the endorsement of the Chancellor’s Administrative Council in hand, IRCC has commissioned several working groups to begin the evolutionary implementation process. IRCC is usually represented on these working groups, but their membership is broadly representative of all interested constituencies.

One group is concerned with the scope, integrity, and presentation of “official” institutional information, such as financial and enrollment data. A different group is coordinating departmental and special-interest Web pages that are deployed primarily for academic market-

“The presentation/discussion meetings revealed that people have a hard time ‘getting into’ a discussion about something that is abstract and outside their experiences.”

**Conclusion**

The overall goals of UNC–CH’s policy framework are (1) to educate the University community to the opportunities and obligations inherent in a pervasive digital networked environment, and (2) to make information as accessible and useful as possible to the University’s various constituencies. These goals can be met only if individual units are guided by a consistent philosophical framework for establishing policies and practices. The IRCC central management partnership representing information resources and information technologies successfully navigated UNC–CH’s highly decentralized and complex environment to produce a policy framework that has coalesced fragmented interest in the role of digital information and information technologies into a healthy community of interest and action.

**For further reading:**


Frost, Renee Woodten, and John Gohsman. “Implementing a Data Administration Function and Strategic Data Planning at the University of Michigan.” CAUSE/EFFECT, Fall 1993, pp. 37-46.


APPENDIX A
A Policy Framework for the University’s Network

Electronic Rights and Responsibilities
at the University of North Carolina at Chapel Hill

The University develops and manages a physical and social learning infrastructure to the economic, social, and cultural benefit of the state and the nation. This learning infrastructure increasingly depends on information in digital form and on digital technologies for communicating, sharing, and analyzing such information. Indeed, digital infrastructure is fast becoming a prerequisite, not only for a more effective and efficient University, but for a better informed and more responsible citizenry.

For example, a centrally supported digital network provides a means to publish much of the University’s official, institutional information for the benefit of both the University and the public. The University, acting through its central administration, is responsible for this information, but centrally coordinated infrastructure and guidelines for publication shift the locus of responsibility for publication and stewardship to the academic and administrative departments that are the sources of most of the information. Similarly, the central administration and academic and administrative units share responsibility for the hardware and software used by the University community to analyze institutional information and other information accessible through the network. Digital infrastructure thus becomes a primary medium in a federal model for balancing responsibilities and encouraging collaboration and public service.

This federal model enables, and the University is committed to, an open flow of information within the University and between the University and the public. The Information Resources Coordinating Council, as the font and guardian of this philosophy, coordinates the development and management of the implied centrally supported digital infrastructure and related services. The Council also formulates the institutional policies that frame the related rights and responsibilities of the institution, those who serve it, and those whom it serves. All members of the University community are responsible, along with the institution, for good citizenship and informed stewardship in a digital democracy. The Council prepared this document to describe these institutional and individual rights and responsibilities and to provide a framework for governing the University’s digital infrastructure and implementing the operational practices that determine its utility to the University and the public.

I. THE NATURE AND PURPOSE OF THE UNIVERSITY’S NETWORK

The network

The University of North Carolina at Chapel Hill operates, through its central administrative offices, a wide-area (inter-building) digital transport network that interconnects local-area networks operated by academic and administrative departments that have agreed to adhere to the University’s Uniform Wiring Policy and to the network management policies coordinated by the Office of Information Technology. The resulting network of networks is the “University’s network.” It is one of the institutionally-operated networks that make up the global Internet and that adhere to the open standards and protocols adopted by the Internet Engineering Task Force. In addition to an Internet gateway, the University’s network also includes a gateway to the North Carolina Information Highway. Through its gateways to the Internet and the North Carolina Information Highway, the University’s network becomes an extended global network that provides access to information and information processing technologies, only a fraction of which is under the stewardship of the University. This extended network and the resources accessible through it serve two primary purposes in the framework of the University’s mission.

✓ To enhance institutional effectiveness and efficiency

By having access to the University’s network and its resources, to include its gateways to the Internet and the North Carolina Information Highway, the faculty, the staff, and the student body can communicate and collaborate among themselves and with their counterparts elsewhere who can connect to the Internet or the North Carolina Information Highway. Network connections are a starting point for internal collaboration and efficiencies, for extending the reach of the University, and for expanding the resources available to the faculty, the staff, and the student body. But the University’s network is a powerful lever for institutional effectiveness and efficiency only to the extent that network connections are easily established and broadly available, are accompanied by easy-to-use services and accessible and reliable mission-critical information, and are based on the standards that guide the development of the Internet and the North Carolina Information Highway.

✓ To publish institutional information about the University

The network’s gateways to the Internet and the North Carolina Information Highway are the primary means by which the University meets its responsibility to the public to publish much of its institutional information in useful
digital formats. By publishing this information via the University’s network, mostly in the form of institutional databases, the University not only meets a public obligation, but serves its own goal of continuous quality improvement in a distributed management model that depends on the free flow of information and that is essential to academic effectiveness. Institutional information, whether for the public or for internal purposes, therefore is published online in an open, democratic framework designed to encourage (1) consistent and ready, affordable access to digital information, (2) stability and reliability from the inquirer’s perspective, (3) integration among disparate databases with minimal duplication in capturing, storing, and maintaining these databases, (4) useful, unifying perspectives on the University’s programs and resources, and (5) information literacy and the use of institutional data in decision making.

II. CONNECTIONS TO THE UNIVERSITY’S NETWORK

Centrally supported connections for the faculty, the staff, and the student body

Members of the faculty, staff, and student body have the right to connect to the University’s network and, through it, the Internet and the North Carolina Information Highway. This right and the resulting right to the University’s information services and applications described in Section III carry the responsibilities that attach to the use of any University resource. Any revocation of any of these rights, in whole or in part, is subject to the normal due process available to any member of the faculty, staff, and student body.

The University centrally provides two fundamental modes of connection for the faculty, staff, and student body: (1) direct connection via Internet protocols through reasonably convenient, centrally supported computer labs on campus, and (2) dial-up connection via a centrally operated pool of modems connected to the switched public telecommunications network through Southern Bell’s Chapel Hill Exchange—to accommodate those who have a computer, a modem, and telephone service and who find themselves in circumstances that do not allow direct connections.

Departmentally supported connections for the faculty, the staff, and the student body

The University’s academic and administrative departments have the right to connect their computers and local-area networks to the University’s network provided that they agree to adhere to the University’s Uniform Wiring Policy and to the Internet-compliant network management policies coordinated by the Office of Information Technology. Departmental connections provide an additional route by which some members of the faculty, staff, and student body connect to the University’s network. Those eligible to exercise such rights of connection as are granted by a department assume responsibilities imposed by the department, which must include the responsibilities described in the first paragraph of this section as applying to those who employ centrally provided connections.

Centrally supported connections for the public

One of the reasons that the University operates gateways to the Internet and the North Carolina Information Highway is to provide mechanisms for the public to connect to the University’s network, primarily to give the public a standards-based interactive digital path into the University’s published institutional information. This means that anyone anywhere with a connection to either the Internet or the North Carolina Information Highway, whether through a commercial online service or otherwise, also has a connection to the University’s network and thereby has access to a vast collection of the University’s institutional information in a useful digital form. The University, however, has no obligation, beyond that to its faculty, staff, and students described in the preceding two paragraphs, to connect individuals and organizations to the Internet or the North Carolina Information Highway.

III. INFORMATION SERVICES AND APPLICATIONS

Information services and applications for the faculty, the staff, and the student body

Members of the faculty, staff, and student body who connect directly or through one of the University’s dial-up lines to the University’s network have the right to, and easy access to, a collection of centrally supported, standards-based network applications and services for (1) communicating with others via the Internet (using Internet-based e-mail and news groups, for example) and (2) locating, retrieving, storing, publishing, and analyzing the University’s published institutional information on the University’s network. These centrally supported standards, applications, and services are deployed to provide ease of connection and use and to comply with, and contribute to, the direction of the Internet and the North Carolina Information Highway. This maximizes the probability that any resource on these extended networks will be readily accessible through the University’s network to any member of the faculty, the staff, or the student body who is eligible to use it. It also helps to ensure that the University’s resources will be accessible, as appropriate, to other networks and computers connecting to the University’s network through the Internet or the North Carolina Information Highway. The University thus draws on the resources of the larger networking community and contributes to it.

The University’s network is a large capital investment incurring very substantial continuing operating costs. Nevertheless, the marginal costs of centrally providing a connection and basic services to any member of the faculty,
staff, and student body are currently negligible, and so the University centrally levies no individual per-use charges. Accordingly, connections and basic services are provided to the faculty, staff, and student body in a context not unlike that defining the use of University-owned telephones to make telephone calls within the Chapel Hill Exchange area. Basic connections and services (1) are reasonably convenient and free to responsible members of the University community, and (2) are the portals to extended services, some of which incur individual per-use charges that are paid in a variety of ways.

Information services and applications for the public
The University also grants access rights on an as-is basis to its published institutional information and to selected software resources on its network to anyone anywhere with a connection to the Internet or to the North Carolina Information Highway. Such information includes, but is not limited to (1) information about the University and its policies, resources, demographics, and management as maintained in institutional databases, and (2) selected academic resources in digital form, to include the catalogs of the University’s libraries in the form of the Online Public Access Catalog operated by the Triangle Research Libraries Network. To advance the University’s mission, other digital information and resources also are available on a selective basis to anyone with a connection to the University’s network, but the University has no general responsibility in this regard. Access to information may be constrained, for example, by commercial licensing agreements. At the other extreme, free access to information may derive from cooperative arrangements between University departments and federal and state agencies. For instance, all official documents of the Clinton administration currently are online on the University’s network as a service to the global Internet community.

The University is aggressive in publishing its institutional information and other important information resources on its network for public access. Within the terms of software licenses and other resource constraints, the University also chooses to provide access to standards-based software tools that allow inquirers to locate, display, capture, and analyze published information. In designing and publishing its digital databases, the University makes every effort to comply with the law by protecting that information which by law is protected from disclosure and by disclosing that information which by law is public. In designing data formats and applications for publishing information online in a way that optimizes the usefulness of vast stores of raw digital data, the University makes no distinction between access by the public and access by members of the faculty, staff, and student body. The design philosophy seeks to provide any inquirer with relational flexibility in aggregating data and spotting trends but, through aggregation, to protect data elements that by reasonable management and community standards would be considered private—an individual’s salary, for example.

Any University-owned computer or local-area network connected to the University’s network provides a means to share mission-related digital information or resources with the public through the gateways to the Internet and the North Carolina Information Highway. The University assumes the responsibility for ensuring that such information is published in digital form by requiring its departments to assume responsibility for the institutional information that they generate. As the steward for institutional data that it collects, a department must comply with the University-wide standards and implementation guidelines overseen by the Information Resources Coordinating Council.

IV. PRIVACY, CONFIDENTIALITY, AND FREEDOM OF EXPRESSION

The University expects members of the faculty, staff, and student body to become familiar with individual and institutional responsibilities to protect confidential information and with the risks to privacy inherent in digital technologies. Good citizenship implies familiarity with the possible states of dynamic digital streams sent or received via the University’s network and static digital files stored on University property. For example, digital streams constituting e-mail communications might traverse public and private networks over which the University has no authority, and they might be broadcast or duplicated by a recipient without the permission of the sender. Just as with printed documents, the University owns and archives digital communications having the official sanction of a department. Otherwise, the University considers static digital files and dynamic digital streams to be private and does not disclose their contents, except as required by contractual obligation or state or federal law. To ensure reliability, however, the University reserves the right to employ backup, storage, and recovery systems throughout its digital infrastructure.

University departments that serve as stewards of an information resource available to the University community at no charge and without contractual obligations have the right, within the limits of prevailing laws, to store the details of any inquiry to, or use of, the information resource. This right can be practiced, however, only if the inquirer is notified at the time of connection of the intent to store any identifying details of the would-be transaction and is given the option to disconnect immediately with confidentiality preserved.

The University respects encryption rights on its network and may itself encrypt information and transactions when secure confidentiality is an obligation.

All existing guarantees of freedom of expression extend to those who use the University’s network as a medium of expression.