Academic Freedom and Electronic Communications

This report, prepared by a subcommittee of the Association's Committee A on Academic Freedom and Tenure, was approved by Committee A and adopted by the Association's Council in November 2004.

The advent of electronic and digital communication as an integral part of academic discourse has profoundly changed the ways in which universities and their faculties pursue teaching and scholarship. Such changes are manifest in the methods by which information is obtained and disseminated, the means of storing and retrieving such information, and of course the ways in which professors teach and students learn. While basic principles of academic freedom transcend even the most fundamental changes in media, recent developments require a re-examination of the application and implications of such principles in a radically new environment.

One overriding principle should shape any such review: Academic freedom, free inquiry, and freedom of expression within the academic community may be limited to no greater extent in electronic format than they are in print, save for the most unusual situation where the very nature of the medium itself might warrant unusual restrictions—and even then only to the extent that such differences demand exceptions or variations. Such obvious differences between old and new media as the vastly greater speed of digital communication, and the far wider audiences that electronic messages may reach, would not, for example, warrant any relaxation of the rigorous precepts of academic freedom. The changes in medium, profound though they are, herald what may be even more basic changes, from familiar and tangible physical space to intangible virtual space.

Several specific issues do, however, deserve attention—not so much because the new media differ sharply from the older and more familiar media, but more because college and university policies that were developed for print and telephonic communications may simply not fit (or may fit imperfectly) the new environment. Analysis of these rapidly changing conditions may not only yield clearer understanding of the need for adaptation, but also help to shape policies better suited to the digital environment, while protecting academic freedom as fully as the precepts they modify and even supersede.

1. Freedom of Research and Publication

The basic precept in the 1940 *Statement of Principles on Academic Freedom and Tenure* that "teachers are entitled to full freedom in research and in the publication of the results" applies with no less force to the use of electronic media for the conduct of research and the dissemination of findings and results than it applies to the use of more traditional media. Two special concerns may, however, occasion slightly different treatment and might cause the modification of policies.

Access To Information In Digital Format

Ensuring unfettered faculty access to print-format materials (e.g., in library collections of monographs and journals) is seldom a concern; universities rarely limit or restrict the availability to faculty of such materials. Access to certain materials in digital form may, however, present different problems. Several universities did in the mid- and late 1990s attempt to curtail access, through the campus computer network, to certain sexually explicit graphics (e.g., “alt.sex” newsgroups) under conditions in which access to comparable print images would be routine. The Virginia General Assembly enacted in 1996 a law that specifically forbade state employees (including all professors at Virginia public institutions) from using state-owned or -leased computers to gain access to sexually explicit materials—at least without receiving explicit permission from a “superior” for a “bona fide research purpose.” Although no other state appears to have imposed comparably draconian limits on access, Virginia’s law was eventually sustained by a federal appeals court despite vigorous legal challenges by six professors, who persuaded a trial judge that the law abridged First Amendment freedoms.

To the extent that a university may respond to such constraints as did the University of Virginia—essentially by granting dispensations to all academic areas on the premise that specific faculty requests for access would indeed reflect “bona fide research purposes”—the vital interests of academic freedom would be best protected against such regrettable intrusions as those imposed by statute on Virginia’s public institutions.

There may be other exceptions, but they can only be noted, not developed fully. For example, seeking access to material protected by the laws of intellectual property may also pose special considerations, about which users might well be cautioned. Institutional policies should identify clearly any such restrictions or limitations on faculty access that the institution deems vital to ensure compliance with federal and state law.

Posting of Unlawful Material

Institutional policy should also address the posting of potentially unlawful material. In many disciplines, scholars may quite legitimately share material that would be deemed “sexually explicit”—art, anatomy, psychology, etc. Such sharing is at least as likely to occur electronically as it has traditionally occurred in print. The difference in medium should no more affect the validity of such exchanges than it should justify a double standard elsewhere. There may, however, be legitimate institutional interests in restricting the range of persons eligible to receive and gain access to such material—especially to ensure that minors are not targeted for images that might lawfully be treated as “harmful to minors.” Any policies designed to protect minors must, however, avoid denying materials to adults who have a valid claim of access—a point that every federal court facing this issue has stressed in the course of striking down at least eight state “harmful to minors on the Internet” laws in recent years.

2. Freedom of Teaching

A basic tenet of the 1940 *Statement of Principles* is that “teachers are entitled to freedom in the classroom in discussing their subject.” The scope of that principle is clear enough in the traditional physical classroom with four walls, a floor, and a ceiling. Increasingly, however, the “classroom” may be a Web page, an electronic bulletin board, a news group, or other electronic medium that clearly has no physical boundaries. Not only do students and professors communicate regularly through e-mail, but much of the material related even to face-to-face classes appears on, and is exchanged through, electronic media. Thus the concept of “classroom” must be broadened to reflect these realities. The “classroom” must indeed encompass all sites where learning occurs—Web sites, home pages, bulletin boards, listservs, etc.[1]

There is, however, one legal caution: A recent state court case (decided on other grounds) raised the potential of professorial abuse of the student-teacher relationship through digital means. Professors might be tempted to post student papers on course Web sites—a practice that should require permission even for print copying and dissemination—and must be sensitive to the vastly greater potential for embarrassment (or worse) to the author by making sensitive personal opinions or information instantly available to a far larger audience. Such risks are magnified many times by an Internet posting, a potential that may warrant one of those few “special rules” for academic discourse in cyberspace.

3. Access to the System: Acceptable-Use Policies

Most colleges and universities have adopted acceptable-use policies governing access to their computing networks and, through those channels, to the Internet. Such policies should not, however, inhibit access to e-mail. No conditions should be imposed upon access to and use of the network more stringent than limits that have been found acceptable for the use of traditional campus channels, unless and to the extent that electronic systems warrant special constraints. Requiring each faculty user to obtain and enter a password is clearly a necessary condition for the functioning of the system, even though print communications impose no counterpart. Moreover, requiring that passwords be kept secret and changed periodically may also be a necessary (if unique) safeguard for a computing network.

More problematic are restrictions such as those that deny the use of the system for “personal matters” or for other than “official university business.” Clearly, computing time is a scarce and valuable resource, priority in the use of which may reasonably reflect the institution’s core mission. Thus some limits may be justified to prevent abuse of the system for extraneous purposes; a ban on the advertising of commercial products and services offers a familiar example. The difficulty with language such as “only official university business,” apart from a distressing lack of precision, is the inherent invitation to selective use of such a standard by an administration anxious to impose substantive constraints on faculty activity. Any restrictions that an institution feels it must impose on “acceptable use” must therefore be clearly and precisely stated, must be content-neutral and narrowly defined, and should address only systemic abuses by users, such as the posting or sending of material that would cause the system to malfunction or would severely inhibit the access of other users.

4. Responsibility in Extramural Utterances

AAUP policy, most notably the 1964 *Committee A Statement on Extramural Utterances,* recognizes that faculty members, speaking as citizens, should be accurate and should "exercise appropriate restraint" as well as show "respect for the opinions of others" in extramural statements. "Extramural utterances," the committee pointed out, "rarely bear upon the faculty member's fitness for continuing service." Whatever problems the physical environment may present for drawing lines between on- and off-campus statements become unmanageable in cyberspace. Are statements posted on a faculty member's home page "intramural" or "extramural"? And does it matter whether a particular statement was entered from the professor's home or office computer—or partly from each? Given these uncertainties, the "extramural utterances" reference simply should not apply to electronic communications, even though the central principles of faculty responsibility to colleagues and community are no less fully applicable in a digital environment. The accident of where a professor happens to be when he or she "utters" a statement bound for the Internet should have no bearing on any judgments made about possible departure from accepted canons of responsibility.

5. Unwarranted Inference of Speaking for or Representing the Institution

The 1940 *Statement* cautions that faculty members "should make every effort to indicate that they are not speaking for the institution" when in fact they are not doing so. The meaning of that constraint is clear enough in the print world. One may refer to one's faculty position and institution "for identification purposes only" in ways that create no tenable inference of institutional attribution. In the digital world, however, avoiding an inappropriate or unwarranted inference may be more difficult. Several years ago, for example, a Northwestern University instructor claimed that a senior colleague's Holocaust-denial statements, posted on the professor's campus-based personal Web page—in contrast to the same statements that had earlier appeared in book form—"make it appear that I and every other [Northwestern] faculty member are a party to what I consider a libel." A California state university was directed to remove from the Web page of a politically active student a strident attack on an incumbent state senator, claimed to violate California's strict ban on any use of state resources for "partisan political purposes." Quite recently, homophobic statements that a university professor posted on his Web log created an analogous concern within the campus community; students who merely sought routine course information and assignments might have been, and occasionally were, exposed to statements some found offensive in ways that would not have happened in the print world.

Institutions may reasonably take steps to avoid such inferences of institutional attribution or complicity, in ways that print communications would not warrant. Disclaimers may be useful, though lawyers often exaggerate the value of such statements. Especially if specific concerns have been raised about material posted on a faculty member's Web page—a Holocaust-denier, or the gay-basher, for example—the poster might preface such material with a clear statement that "material on this Web site does not represent the views of, and has not been reviewed or

approved by, ____ University." Such a disclaimer could also be generalized on the institution's home page, or on the directory by which a visitor to the site would initially explore professorial Web pages or Web logs. No such statement should imply either approval or disapproval but should, consistent with principles of academic freedom, recognize that the individual professor (not the institution) is responsible for his or her views or opinions.

6. Sanctions for Abuse or Misuse: Terminating Electronic Access

Administrations at some institutions appear to have viewed computer and Internet access as a lower-order faculty perquisite that may be summarily terminated. Such views need to be rejected unequivocally. Access to campus computing facilities, and through them to the Internet, represents a vital component of faculty status for most scholars and teachers. Yet it would be naïve to suggest that circumstances might never warrant withdrawal or suspension of digital channels. Access may be denied or limited only for the most serious of reasons (e.g., creating and unleashing on the campus server a destructive virus), and only after the filing of formal charges and the pursuit of rigorous procedures, even where the transgression may not be so grave as to warrant dismissal or suspension. The university's policies must specify with precision the infractions that might warrant such a severe sanction, recognizing only conduct that jeopardizes the system and the access of others—contrasting with a rule still on the books of one major public university that imposes a minimum three-day suspension upon any user found eating in a computer lab—a ban presumably aimed at students, but theoretically applicable to professors as well. The policy should also prescribe the procedures to be followed in such a case. In exigent circumstances, a faculty member's computer access might be summarily and briefly suspended during an investigation of serious charges of abuse or misuse. Any such suspension should be approved by the chief academic officer as well as the chief information technology officer, should be no longer than necessary to conduct the investigation, and should be subject to some form of prior internal faculty review.

7. Freedom of Artistic Expression

AAUP policy elsewhere recognizes that academic freedom includes freedom of artistic expression "in visual and performing arts." Increasingly, artistic expression that challenges conventional tastes and norms does involve digital images, even more than images on canvas, film, or dance. It is thus vital to affirm that academic freedom does include such novel as well as more traditional media. Indeed, much of the recent constitutional litigation over regulation of Internet content has raised precisely such issues. The Supreme Court has struck down congressional bans on "indecency" on the Internet, and on "virtual child pornography," while lower federal courts have consistently invalidated state bans on the Internet posting of "material harmful to minors" in digital form.

8. Campus Speech Codes and Harassment Policies

The AAUP has condemned restrictive speech codes and harassment policies that target speech on the basis of the speaker's viewpoint or message.2 Such condemnation should apply with equal force to regulation of digital or electronic campus speech. Such differences as exist among media do not warrant harsher treatment of threats, slurs, epithets, or harassing language because they occur in digital form. Indeed, it is quite possible that electronic messages are protected to an even greater degree than their print-era counterparts. The doctrine of "fighting words" offers an illustration. While the Supreme Court held many years ago that a speaker could be punished for highly provocative face-to-face utterances likely to trigger a violent response—the definition of "fighting words"—there does not seem to be any basis for treating even the most intemperate digital "flaming" in the same way, since the proximate, "in-your-face" risks simply do not exist when the combatants are seated at keyboards an unknown distance apart. We know far less about the legal status of digital threats; the federal appeals court in California upheld a substantial judgment in favor of abortion-clinic staff members against a group that had posted hateful and threatening statements on the "Nuremberg Web site," the court reasoning that the named abortion providers could reasonably have felt as directly threatened by such messages on a Web site as by similarly menacing language found on a poster or flier or uttered orally. Other cases are pending that may define more sharply the nature and liability of digital threats. The central point here is that campus speech codes and broad verbal harassment rules are no more tolerable when they target digital or electronic hate messages than when they target similarly spiteful print messages.

9. Privacy of Electronic Communications

Institutions of higher learning seem hardly immune from the belief—pervasive in the corporate world—that the level of privacy due to digital communications is substantially lower than what users of more traditional media may expect. In the relatively few judicial tests of this issue, courts seem to accept such a lower standard, even for faculty communications. One federal appeals court recently and illustratively rejected a university professor's electronic-privacy claim, because "the employee was explicitly cautioned that information flowing through or stored in computers within the network cannot be considered confidential, and where computer users were notified that network administrators and others were free to view data downloaded from the Internet." Although the content of the material involved in that case was indefensible—a professor's files of child pornography—such broad judicial pronouncements extend well beyond forbidden material, and dangerously imply an almost dismissive view of privacy claims in the campus as well as in the corporate context.

There are undeniable differences among communications media, which may take some toll on privacy. A college or university computing network legitimately "backs up" some portion of each day's e-mail traffic. Information-technology staff members in the normal course of events have a degree of access to electronic messages that would be unthinkable for personnel in the university mailroom or the campus telephone switchboard. By its very nature, electronic communication incurs certain risks that have no print counterpart—for example, the potential invasion of the system by hackers, despite the institution's best efforts to discourage

such intrusions. These risks are simply part of the reality of the digital age, and our extensive reliance upon computer networks for the conduct of academic discourse. Yet such claims as university “ownership” of the hardware and telephone lines, or the need to ensure that the university’s business gets done on time, could dangerously diminish the countervailing interests in digital privacy. There are genuine academic freedom concerns that have not yet been recognized by the courts, and that are less than fully or adequately reflected in most institutional policies. The sensitivity of academic communications and the wide range of scholarly purposes for which digital channels are invoked warrant a markedly higher level of protection. A fully responsive policy would reflect at least these criteria:

a. Every college or university should make clear, to all computer users, any exceptions it deems necessary to impose upon the presumed privacy of communications, whether in print or in digital form.

b. There must be substantial and meaningful faculty involvement in the formulation of any such exceptions (e.g., requiring formal approval or endorsement by a faculty senate or comparable governance group).

c. The basic standard for e-mail privacy should be that which is assured to persons who send and receive sealed envelopes through the physical mail system—that envelopes would not be opened by university officials save for exigent conditions (e.g., leaking of a noxious chemical or ticking or other indicia of an explosive).

d. If a need arises to divert or intercept a private e-mail message to or from a faculty member, both the sender and the recipient should be notified in ample time for them to pursue protective measures—save in the rare case where any such delay would create imminent risk to human safety or university property.

e. The contents of any such messages that have been diverted or intercepted may not be used or disseminated more widely than the basis for such exceptional action may warrant.

f. Should the occasion ever arise to suspend or terminate an individual faculty member’s access to the computer system, so drastic a step should be taken only in response to a serious threat to the system, and should be preceded by a hearing before a faculty committee on the specific charge or charges of misuse or abuse.

g. Finally, similar safeguards should be fashioned (with full and meaningful faculty involvement in that process) and applied to other facets of electronic communications within the campus community—for example, the posting of sensitive evaluations or course materials, whose confidentiality may prove harder to maintain than might initially be supposed. Careful consideration should be given to privacy needs in myriad situations where unauthorized disclosure of electronic messages and materials could jeopardize personal reputations and other vital interests, and could ultimately deter free and open communications within the campus community.

Such principles as these, designed as they are to ensure privacy of electronic communications, will require careful and extensive study by each institution, and the tailoring of specific responses consistent not only with institutional needs and values, but also with state and local law. This report is designed to facilitate that process.

Notes

1. For a more comprehensive treatment of teaching at a distance, see the Association's 1999 "Statement on Distance Education," *Policy Documents and Reports,* 10th ed. (Washington, D.C.: AAUP, 2006), 211–13. Back to text

2. See the AAUP's statements "On Freedom of Expression and Campus Speech Codes," *Policy Documents and Reports,* 37–38, and "Sexual Harassment: Suggested Policy and Procedures for Handling Complaints," ibid., 244–46. Back to text

Academic Freedom and Electronic Communications

This report was prepared by a subcommittee of the Association's CommitteeA on Academic Freedom and Tenure and initially published in 1997. A revised text was approved by Committee A and adopted by the Association's Council in November 2004.

The advent of electronic and digital communication as an integral part of academic discourse has profoundly changed the ways in which universities and their faculties pursue teaching and scholarship. Such changes are manifest in the methods by which information is obtained and disseminated, the means of storing and retrieving such information, and of course the ways in which professors teach and students learn. While basic principles of academic freedom transcend even the most fundamental changes in media, recent developments require a re-examination of the application and implications of such principles in a radically new environment.

One overriding principle should shape any such review: Academic freedom, free inquiry and freedom of expression within the academic community may be limited to no greater extent in electronic format than they are in print, save for the most unusual situation where the very nature of the medium itself might warrant unusual restrictions—and even then only to the extent that such differences demand exceptions or variations. Such obvious differences between old and new media as the vastly greater speed of digital communication, and the far wider audiences that electronic messages may reach, would not, for example, warrant any relaxation of the rigorous precepts of academic freedom. The changes in medium, profound though they are, herald what may be even more basic changes, from familiar and tangible physical space to intangible virtual space.

Several specific issues do, however, deserve attention—not so much because the new media differ sharply from the older and more familiar media, but more because college and university policies that were developed for print and telephonic communications may simply not fit (or may fit imperfectly) the new environment. Analysis of these rapidly changing conditions may not only yield clearer understanding of the need for adaptation, but also help to shape policies better suited to the digital environment, while protecting academic freedom as fully as the precepts they modify and even supersede.

1. Freedom of Research and Publication.

The basic precept in the 1940 *Statement of Principles on Academic Freedom and Tenure* that "teachers are entitled to full freedom in research and in the publication of results" applies with no less force to the use of electronic media for the conduct of research and the dissemination of findings and results than it applies to the use of more traditional media. Two special concerns may, however, occasion slightly different treatment and might cause the modification of policies.

Access to information in digital format. Ensuring unfettered faculty access to print format materials (e.g., in library collections of monographs and journals) is seldom a concern; universities rarely limit or restrict the availability to faculty of such materials. Access to certain materials in digital form may, however, present different problems. Several universities did in the mid- and late 1990s attempt to curtail access, through the campus computer network, to certain sexually explicit graphics (e.g., "alt.sex" newsgroups) under conditions in which access to comparable print images would be routine. The Virginia General Assembly enacted in 1996 a law which specifically forbade state employees (including all professors at Virginia public institutions) from using state-owned or -leased computers to gain access to sexually explicit materials - at least without receiving explicit permission from a "superior" for a "bona fide research purpose." Although no other state appears to have imposed comparably draconian limits on access, Virginia's law was eventually sustained by a federal appeals court despite

vigorous legal challenges by six professors, who persuaded a trial judge that the law abridged First Amendment freedoms.

To the extent that a university may respond to such constraints as did the University of Virginia—essentially by granting dispensations to all academic areas on the premise that specific faculty requests for access would indeed reflect "bona fide research purposes"—the vital interests of academic freedom would be best protected against such regrettable intrusions as those imposed by statute on Virginia's public institutions.

There may be other exceptions but they can only be noted, not developed fully. For example, seeking access to material protected by the laws of intellectual property may also pose special considerations, about which users might well be cautioned. Institutional policies should identify clearly any such restrictions or limitations on faculty access that the institution deems vital to ensure compliance with federal and state law.

Posting of unlawful material. Institutional policy should also address the posting of potentially unlawful material. In many disciplines, scholars may quite legitimately share material that would be deemed "sexually explicit"—art, anatomy, psychology, etc. Such sharing is at least as likely to occur electronically as it has traditionally occurred in print. The difference in medium should no more affect the validity of such exchanges than it should justify a double standard elsewhere. There may, however, be legitimate institutional interests in restricting the range of persons eligible to receive and gain access to such material—especially to ensure that minors are not targeted for images that might lawfully be treated as "harmful to minors." Any policies designed to protect minors must, however, avoid denying materials to adults who have a valid claim of access - a point that every federal court facing this issue has stressed in the course of striking down at least eight state "harmful to minors on the Internet" laws in recent years.

2. Freedom of Teaching.

A basic tenet of the 1940 *Statement of Principles* is that "teachers are entitled to freedom in the classroom in discussing their subject." The scope of that principle is clear enough in the traditional physical classroom with four walls, a floor and a ceiling. Increasingly, however, the "classroom" may be a Web page, an electronic bulletin board, a news group, or other electronic medium that clearly has no physical boundaries. Not only do students and professors communicate regularly through e-mail, but much of the material related even to face-to-face classes appears on, and is exchanged through, electronic media. Thus the concept of "classroom" must be broadened to reflect these realities. The "classroom" must indeed encompass all sites where learning occurs—websites, home pages, bulletin boards, list-serves, etc.[1]

There is, however, one legal caution: A recent state court case (decided on other grounds) raised the potential of professorial abuse of the student-teacher relationship through digital means. Professors might be tempted to post student papers on course Web sites—a practice that should require permission even for print copying and dissemination—and must be sensitive to the vastly greater potential for embarrassment (or worse) to the author by making sensitive personal opinions or information instantly available to a far larger audience. Such risks are magnified many times by an Internet posting, a potential which may warrant one of those few "special rules" for academic discourse in cyberspace.

3. Access to the System: Acceptable Use Policies.

Most colleges and universities have adopted acceptable use policies governing access to their computing networks and, through those channels, to the Internet. Such policies should not, however, inhibit access to e-mail. No conditions should be imposed upon access to and use of the network more stringent than limits that have been found acceptable for the use of traditional campus channels, unless and to the extent that electronic systems warrant special constraints.

Requiring each faculty user to obtain and enter a password is clearly a necessary condition for the functioning of the system, even though print communications impose no counterpart. Moreover, requiring that passwords be kept secret and changed periodically may also be a necessary (if unique) safeguard for a computing network.

More problematic are restrictions such as those that deny the use of the system for "personal matters" or for other than "official university business." Clearly, computing time is a scarce and valuable resource, priority in the use of which may reasonably reflect the institution's core mission. Thus some limits may be justified to prevent abuse of the system for extraneous purposes; a ban on the advertising of commercial products and services offers a familiar example. The difficulty with language such as "only official university business," apart from a distressing lack of precision, is the inherent invitation to selective use of such a standard by an administration anxious to impose substantive constraints on faculty activity. Any restrictions which an institution feels it must impose on "acceptable use" must therefore be clearly and precisely stated, must be content-neutral and narrowly defined, and should address only systemic abuses by users, such as the posting or sending of material which would cause the system to malfunction or would severely inhibit the access of other users.

4. Responsibility in Extramural Utterances.

AAUP policy, most notably the 1964 "Committee A Statement on Extramural Utterances," recognizes that faculty members, speaking as citizens, should be accurate and should "exercise appropriate restraint" as well as show "respect for the opinions of others" in extramural statements. "Extramural utterances," the committee pointed out, "rarely bear upon the faculty member's fitness for continuing service." Whatever problems the physical environment may present for drawing lines between on- and off-campus statements become unmanageable in cyberspace. Are statements posted on a faculty member's home page "intramural" or extramural"? And does it matter whether a particular statement was entered from the professor's home or office computer—or partly from each? Given these uncertainties, the "extramural utterances" reference simply should not apply to electronic communications, even though the central principles of faculty responsibility to colleagues and community are no less fully applicable in a digital environment. The accident of where a professor happens to be when he or she "utters" a statement bound for the Internet should have no bearing on any judgments made about possible departure from accepted canons of responsibility.

5. Avoiding An Unwarranted Inference of Speaking for or Representing the Institution.

The 1940 *Statement* cautions that faculty members "should make every effort to indicate that they are not speaking for the institution" when in fact they are not doing so. The meaning of that constraint is clear enough in the print world. One may refer to one's faculty position and institution "for identification purposes only" in ways that create no tenable inference of institutional attribution. In the digital world, however, avoiding an inappropriate or unwarranted inference may be more difficult. Several years ago, for example, a Northwestern University instructor claimed that a senior colleague's Holocaust-denial statements, posted on the professor's campus-based personal Web page—in contrast to the same statements that had earlier appeared in book form—"make it appear that I and every other [Northwestern] faculty member are a party to what I consider a libel." A California state university was directed to remove from the Web page of a politically active student a strident attack on an incumbent state senator, claimed to violate California's strict ban on any use of state resources for "partisan political purposes." Quite recently, homophobic statements that a university professor posted on his weblog created an analogous concern within the campus community; students who merely sought routine course information and assignments might have been, and occasionally were, exposed to statements some found offensive in ways that would not have happened in the print world.

Institutions may reasonably take steps to avoid such inferences of institutional attribution or complicity, in ways that print communications would not warrant. Disclaimers may be useful, though lawyers often exaggerate the value of such statements. Especially if specific concerns have been raised about material posted on a faculty member's Web page—a Holocaust-denier, or the gay-basher, for example— the poster might preface such material with a clear statement that "material on this Web site does not represent the views of, and has not been reviewed or approved by, ____ University." Such a disclaimer could also be generalized on the institution's home page, or on the directory by which a visitor to the site would initially explore professorial Web pages or Web logs. No such statement should imply either approval or disapproval but should, consistent with principles of academic freedom, recognize that the individual professor (not the institution) is responsible for his or her views or opinions.

6. Sanctions for Abuse or Misuse: Terminating Electronic Access.

Administrations at some institutions appear to have viewed computer and Internet access as a lower-order faculty perquisite that may be summarily terminated. Such views need to be rejected unequivocally. Access to campus computing facilities, and through them to the Internet, represents a vital component of faculty status for most scholars and teachers. Yet it would be naïve to suggest that circumstances might never warrant withdrawal or suspension of digital channels. Access may be denied or limited only for the most serious of reasons (e.g., creating and unleashing on the campus server a destructive virus), and only after the filing of formal charges and the pursuit of rigorous procedures, even where the transgression may not be so grave as to warrant dismissal or suspension. The university's policies must specify with precision the infractions that might warrant such a severe sanction, recognizing only conduct that jeopardizes the system and the access of others—contrasting with a rule still on the books of one major public university that imposes a minimum three-day suspension upon any user found eating in a computer lab—a ban presumably aimed at students, but theoretically applicable to professors as well. The policy should also prescribe the procedures to be followed in such a case. In exigent circumstances, a faculty member's computer access might be summarily and briefly suspended during an investigation of serious charges of abuse or misuse. Any such suspension should be approved by the chief academic officer as well as the chief information technology officer, should be no longer than necessary to conduct the investigation, and should be subject to some form of prior internal faculty review.

7. Freedom of Artistic Expression.

AAUP policy elsewhere recognizes that academic freedom includes freedom of artistic expression "in visual and performing arts." Increasingly, artistic expression that challenges conventional tastes and norms does involve digital images, even more than images on canvas, film or dance. It is thus vital to affirm that academic freedom does include such novel as well as more traditional media. Indeed, much of the recent constitutional litigation over regulation of Internet content has raised precisely such issues. The Supreme Court has struck down Congressional bans on "indecency" on the Internet, and on "virtual child pornography," while lower federal courts have consistently invalidated state bans on the Internet posting of "material harmful to minors" in digital form.

8. Campus Speech Codes and Harassment Policies.

The AAUP has condemned restrictive speech codes and harassment policies that target speech on the basis of the speaker's viewpoint or message.[2] Such condemnation should apply with equal force to regulation of digital or electronic campus speech. Such differences as exist among media do not warrant harsher treatment of threats, slurs, epithets, or harassing language because they occur in digital form. Indeed, it is quite possible that electronic messages are protected to an even greater degree than their print-era counterparts. The doctrine of "fighting words" offers an illustration. While the Supreme Court held many years ago that a speaker could be punished for highly provocative face-to-face utterances likely to trigger a violent response - the definition of "fighting words"—there does not seem to be any basis for

treating even the most intemperate digital "flaming" in the same way, since the proximate, "in-your-face" risks simply do not exist when the combatants are seated at keyboards an unknown distance apart. We know far less about the legal status of digital threats; the federal appeals court in California upheld a substantial judgment in favor of abortion-clinic staff members against a group that had posted hateful and threatening statements on the "Nuremberg Web site," the court reasoning that the named abortion providers could reasonably have felt as directly threatened by such messages on a Web site as by similarly menacing language found on a poster or flier or uttered orally. Other cases are pending which may define more sharply the nature and liability of digital threats. The central point here is that campus speech codes and broad verbal harassment rules are no more tolerable when they target digital or electronic hate messages than when they target similarly spiteful print messages.

9. Privacy of Electronic Communications.

Institutions of higher learning seem hardly immune from the belief—pervasive in the corporate world—that the level of privacy due to digital communications is substantially lower than what users of more traditional media may expect. In the relatively few judicial tests of this issue, courts seem to accept such a lower standard, even for faculty communications. One federal appeals court recently and illustratively rejected a university professor's electronic privacy claim, because "the employee was explicitly cautioned that information flowing through or stored in computers within the network cannot be considered confidential, and where computer users were notified that network administrators and others were free to view data downloaded from the Internet." Although the content of the material involved in that case was indefensible—a professor's files of child pornography —such broad judicial pronouncements extend well beyond forbidden material, and dangerously imply an almost dismissive view of privacy claims in the campus as well as in the corporate context.

There are undeniable differences among communications media, which may take some toll on privacy. A college or university computing network legitimately "backs up" some portion of each day's e-mail traffic. Information technology staff members in the normal course of events have a degree of access to electronic messages that would be unthinkable for personnel in the university mailroom or the campus telephone switchboard. By its very nature, electronic communication incurs certain risks that have no print counterpart—for example, the potential invasion of the system by hackers, despite the institution's best efforts to discourage such intrusions. These risks are simply part of the reality of the digital age, and our extensive reliance upon computer networks for the conduct of academic discourse. Yet such claims as university "ownership" of the hardware and phone lines, or the need to ensure that the university's business gets done on time, could dangerously diminish the countervailing interests in digital privacy. There are genuine academic freedom concerns that have not yet been recognized by the courts, and that are less than fully or adequately reflected in most institutional policies. The sensitivity of academic communications and the wide range of scholarly purposes for which digital channels are invoked warrant a markedly higher level of protection. A fully responsive policy would reflect at least these criteria:

- Every college or university should make clear, to all computer users, any exceptions it deems necessary to impose upon the presumed privacy of communications, whether in print or in digital form.

- There must be substantial and meaningful faculty involvement in the formulation of any such exceptions (for example, requiring formal approval or endorsement by a faculty senate or comparable governance group).

- The basic standard for e-mail privacy should be that which is assured to persons who send and receive sealed envelopes through the physical mail system— that envelopes would not be opened by university officials save for exigent conditions (e.g., leaking of

a noxious chemical, ticking or other indicia of an explosive, etc).

- If a need arises to divert or intercept a private e-mail message to or from a faculty member, both the sender and the recipient should be notified in ample time for them to pursue protective measures—save in the rare case where any such delay would create imminent risk to human safety or university property.

- The contents of any such messages that have been diverted or intercepted may not be used or disseminated more widely than the basis for such exceptional action may warrant.

- Should the occasion ever arise to suspend or terminate an individual faculty member's access to the computer system, so drastic a step should be taken only in response to a serious threat to the system, and should be preceded by a hearing before a faculty committee on the specific charge or charges of misuse or abuse.

  Finally, similar safeguards should be fashioned (with full and meaningful faculty involvement in that process) and applied to other facets of electronic communications within the campus community—for example, the posting of sensitive evaluations or course materials, as to whose confidentiality may prove harder to maintain than might initially be supposed. Careful consideration should be given to privacy needs in myriad situations where unauthorized disclosure of electronic messages and materials could jeopardize personal reputations and other vital interests, and could ultimately deter free and open communications within the campus community.

Such principles as these, designed as they are to ensure privacy of electronic communications, will require careful and extensive study by each institution, and the tailoring of specific responses consistent not only with institutional needs and values, but also with state and local law. This report is designed to facilitate that process.

Notes

1. For a more comprehensive treatment of teaching at a distance, *see* the Association's 1999 "*Statement on Distance Education," AAUP Policy Documents and Reports*, 9th ed. (Washington, D.C., 2001): 179-81. Back to text.

2. *See* AAUP's statement "*On Freedom of Expression and Campus Speech Codes*," *Policy Documents and Reports*, 37-38, and "Sexual Harassment: Suggested Policy and Procedures for Handling Complaints," ibid., 20