Swarthmore College
Policy Regarding Preservation of Privacy and Confidentiality of Records

As approved by the Faculty on April 29, 2005

1. Privacy is more than a concern with keeping personal matters personal. When privacy is wrongly compromised, freedom of thought, expression, and action are seriously eroded. This is especially true in an academic setting, where students and faculty are exploring ideas and modes of expression. But privacy is a concern for all members of the College community.

2. In a college community, students, faculty members, and staff will learn much about the ideas and beliefs of one another. This process should not be contaminated by the fear that ideas and beliefs, expressions and convictions, are being surreptitiously monitored or systematically reported to persons or agencies inside or outside the community. Intellectual freedom and mutual trust are indispensable to one another. In classrooms and seminars, in informal discussions in dormitories, dining rooms, and libraries, members of the College community should be free to adventure in ideas and expression.

3. Through its policy, Swarthmore College strives to reconcile sometimes competing concerns. Paramount is not to compromise the College’s fundamental educational mission: to sustain a lively intellectual and social community of students, faculty, and staff. But against this must be balanced concerns that engage issues of civility, efficiency, legality, security, and supportive working conditions. Thus the individual right to privacy, though stringent and broad, is neither absolute nor unlimited. In particular, under guidelines established by the President acting on behalf of the Board of Managers, as having the authority to do so, certain supervisors and administrators, as designated herein, may access an individual’s documents, communications, contacts and materials in cases of clear functional need to insure the efficient and responsible functioning of the College in the pursuit of its mission. This need extends to the proper assurance of a supportive – safe as well as nurturing – environment in which to learn and do one’s work. Accordingly, those in supervisory positions, like those involved with assuring the College’s compliance with legal requirements, must be entitled to take appropriate measures in circumstances relating to functional need. Equally, the administrators of the College’s various computer systems must be entitled to take appropriate actions in circumstances related to the need to insure that these systems function safely, efficiently, and securely, as is required to

1 What follows is intended to replace the entire section of the Faculty Handbook on p. 25 of the 2001 edition; i.e., section 2. Ideas and Information, under II. ACADEMIC AND ADMINISTRATIVE POLICIES AND PROCEDURES, II-A. GENERAL POLICIES, 4. PRESERVATION OF PRIVACY AND CONFIDENTIALITY OF RECORDS, a. Privacy of Students, Faculty, Staff. Numbering is here for convenience only, and will not appear in the Handbook itself.

2 “Administrator:” anyone (member of the faculty or staff, or student) having responsibility for insuring the proper operation of a computing system, including any individual to whom such responsibility is delegated by a responsible supervisor. “Supervisor:” anyone (member of the faculty or staff, or student) who is responsible for supervising the work of some other individual or individuals.
support the College’s educational mission. Those who take such measures under this policy have an obligation, if asked by those affected, to justify their actions in terms of functional need.

4. Except where required by law or clear functional need, the communications system of the College, including telephone, mail, e-mail, and computing facilities, may not be used for surveillance. Messages to and from members of the College community may not be intercepted or monitored, nor information about the origin or destination of messages collected, except as functional need requires as specified in the provisions that follow. Information fortuitously gained by those operating the communications system or in College facilities may not be passed on to others in any form, unless a violation of the law or of College regulations is suspected or apparent, in which case appropriate College authorities are to be notified.

5. Swarthmore College provides faculty, students, and many employees with access to computers and electronic systems, including e-mail and Internet access, for (a) educational and research purposes and (b) to conduct the College’s business. While Swarthmore College does not monitor the use of these systems and equipment -- except for normal maintenance and to prevent or remedy various electronic attacks -- the systems and computers are the legal property of Swarthmore College. Therefore, the College can be required to provide legal authorities access to equipment and systems. The College will comply with all legal requirements, including any that it regards as an indefensible breach of privacy. In complying, however, it will use reasonable effort to find a way that least transgresses on what it regards as its justifiable policies on privacy, electronic and otherwise. E-mail messages are also, as a matter of law, the legal property of the College. However, in cases of clear functional need (e.g., an internal investigation or an unanticipated absence requiring access) the College has the right to retrieve and/or read the contents of a community member’s computer or electronic communications. Even when it is permissible to retrieve and examine the contents of a computer, the College should not examine anything other than what is required by clear functional need.

6. Except as pertains to the administration of the College and except for matters outlined in this handbook, personal files and information of whatsoever form existing within College computing systems for whatever duration are to be controlled by the user and not accessed by any others without the user’s permission, including College authorities. \(^3\) This includes, but is not limited to, such things as research data, essays, papers, notes, communications (e.g., e-mail and letters), letters of recommendation, legally downloaded material, personally owned and legally permissible software, browser settings, and records. There are inevitable borderline cases that should be resolved in accordance with the principles set forth in this policy. \(^4\)

---

\(^3\) Under the application of various laws governing access by legal authorities to computing and communication facilities, and pursuant to College functional need, the computing systems of Swarthmore College include all computers on or off campus, College owned or not, that are connected, either occasionally or normally, to any College owned or maintained electronic network or are used in the conduct of College business without ever being connected to such a network.

\(^4\) Here is how to resolve two cases:

If a faculty member becomes incapacitated before submitting grades for a current semester, the grades may be retrieved from his or her office or computer. Any notes or comments
7. While the College makes a reasonable effort to protect the confidentiality of electronic communication and the content of computers and storage devices connected to the network, the very nature of the technology makes it impossible for the College to guarantee privacy. Although individuals and the College can each do a great deal to reduce the threat of disclosure of such content, ultimately there is no way to ensure that unintended interception, monitoring, inspection, storage, dissemination, or use of computer and network content can never occur. Any use of the Internet (e.g. email, the WWW, or voice over IP), even simply being connected to the Internet, potentially exposes a computer's content and any of its network communication to inspection, deletion, or other unintended use. It is possible that any communication or content, including that which is deleted, will be illicitly or legally retrieved by others. Therefore, it is each individual’s responsibility to understand the limitations of a networked world and to take great care in keeping private what he or she wishes to keep private.

8. In order for the College’s various electronic systems to support its educational mission and to conduct its business, they should function safely, efficiently, and securely. Administrators of such systems and those in supervisory positions must therefore be entitled to take appropriate measures. Nevertheless, those in such positions must be able to justify their actions if called upon to do so and they have an obligation to act in ways respectful of individual privacy to the extent possible.

9. Different elements of the College community have differing functional needs with respect to computing and computing systems that lead to distinctive modes of implementing the College’s electronic privacy policy. Even within the academic sphere, there are justifiably distinctive policies: Computer Science, for example, uses a much more open system – offering far less privacy – than is typical of the College generally. Several other academic departments also maintain more open, independently networked systems, and faculty in some academic departments may on occasion oversee instructional uses of individual electronic systems. Approaches that make good sense generally, therefore, would not if applied to distinct instructional systems or modes of instruction. Administrators of any distinctive computing system, however, should ensure that its users are fully informed regarding their rights to privacy, or lack thereof, in using the system. (For an example of good practice in this regard, see “The User Agreement” read and signed by all who wish to use the Computer Science system.) Signing a user agreement is not the only way of fully informing users of their rights, privileges, pertaining to a student graded, however, remain private: they are not a required part of submitting grades. Even when the search for grades is permissible, however, it should be done with the Provost’s approval and conducted in the presence of either the Chair or someone designated by the Provost to oversee the search. Any other contents inadvertently found should remain private and confidential, unless so doing would bring with it College legal liability.

Some faculty might wish to have letters of recommendation and other contents available should they be incapacitated or unavoidably absent; others not. Those who do must state in writing what is available for retrieval and what is not, and under what conditions. In the case of letters of recommendation, for example, a faculty member can easily make a copy of such letters and give them to the departmental AA with instructions on how to use them.
and responsibilities; e.g., a clear statement on privacy limitations at the head of a syllabus might suffice.

10. Notwithstanding warranted diversity in the modes of implementing this policy, certain general guidelines that should be followed do apply in all settings.

   a. Intrusive investigations or searches variously undertaken – to ensure efficient functioning, to locate the source of some problem, or to examine suspected misconduct – should be of reasonable duration. This does not preclude further investigation, however, if satisfying the original need justifies further investigation; e.g., when an investigation is of possible continuing wrongdoing or involves tracing potential computer abuses.

   b. The functional need to access individual’s electronic data, files or materials does not justify or excuse any willful, negligent, or reckless disregard of privacy.

   c. Normally, appropriate means, efficiency, and security are complementary and mutually reinforcing. The press of College business might sometimes, however, result in means later deemed excessive. For example, in the midst of a virus attack, ITS might take measures that it reasonably regards as necessary only to conclude after the attack that less intrusive means might have been employed. There is no violation of College policies in such cases.

   d. Similarly, civility is normally complementary to and mutually reinforcing vis-à-vis appropriate means, efficiency, and security. Nevertheless, the immediacy of College business can result in access that bypasses civility. Examples: when there is an investigation of possible illegal misconduct or of abuse of policies involving computing system use; when the College must investigate a security breach; when a staff member is unavailable for some reason; when system administrators determine that a particular computer may be the source of some debilitating network problem. Except in cases of routine maintenance or where imprudent in relation to some on-going investigation of wrong-doing, prior notification should be given of any intrusive investigations or searches. However, prior notification is not always practically possible; in such cases, with exceptions as just noted, post-notification is to be given.

   e. Where reasonable, the least intrusive methods given the context should be used. Similarly, the extent and scope of investigation should be no wider than is reasonably necessary.