Policy on Access to Electronic Information

As voted by the President and Fellows of Harvard College on March 31, 2014; amended May 8, 2015

Scope of Policy

This policy sets out guidelines and processes for University access to user electronic information stored in or transmitted through any University system. This policy applies to all Schools and units of the University.

General Statement

Members of the Harvard community rely on technology in multiple aspects of their work, teaching, research, study, and other activity. In doing so, they use electronic systems, networks, and devices that the University owns, provides, or administers. The University makes these systems available for the purpose of carrying out the University's various activities. To promote trust within the University community, the University should be transparent about its policy regarding the circumstances in which it may access user electronic information stored in or transmitted through these systems. This policy therefore sets out guidelines and processes that apply when the University seeks access to such electronic information, consonant with the University's interest in maintaining an environment in which free academic inquiry thrives. This policy is intended to establish internal standards and procedures governing such access by the University; it is not meant to create rights in any individual to seek legal redress for action inconsistent with the policy.

The policy is grounded on six important principles:

- Access should occur only for a legitimate and important University purpose.
- Access should be authorized by an appropriate and accountable person.
- In general, notice should be given when user electronic information will be or has been accessed.
- Access should be limited to the user electronic information needed to accomplish the purpose.
- Sufficient records should be kept to enable appropriate review of compliance with this policy.
- Access should be subject to ongoing, independent oversight by a committee that includes faculty representation.

Terminology

The following terms are used in this policy with the following meanings:

"University systems" refers to all services, networks, and devices owned, provided, or administered by any unit of the University, such as email services, Internet access, file servers, voice message services, storage devices and services, laptop and desktop computers, phones and other mobile devices, and usage and access logs.

"Users" refers to Harvard faculty, others holding academic appointments at Harvard, students, staff, and other employees.

"User electronic information," for any particular user, refers to:

(i) Documents and communications, including emails, voice mails and text messages, and their associated metadata, which are located in files and accounts associated with a particular user. For example, this would include all emails and their attachments in a user's inbox, sent items folder, or other email folders that are recognized as part of the account associated with that user, and all documents in that user account's document folders; and

(ii) Information generated by automated processes triggered by that user's use of University systems, such as tracks of Internet use and logs of access to facilities.

User electronic information does not include (a) records regularly maintained by the University in the ordinary course of business, such as personnel records or student academic records, or information provided by personnel in connection with regular University record-keeping, such as entries in a University travel registry; or (b) information as described in (ii), above, when accessed by the University without identifying or seeking to identify any particular user.

Contents

I. Reasons for Access

The University does not routinely monitor the content of information transmitted through or stored in University information systems. The University may obtain access to user electronic information in some circumstances, but only for a legitimate institutional purpose. The paragraphs below describe certain purposes for which the University may access such information. While this list is expected to cover most instances of access, the list is not intended to be exhaustive. The University may access user electronic information for comparable reasons that likewise advance a legitimate institutional purpose, as determined by a person designated to authorize access pursuant to this policy and subject to review by the oversight committee as described in Part VI.

Although this policy applies to the electronic information of faculty, staff, and students alike, in evaluating the institutional purpose, the person designated to authorize access should in each case weigh not only the stated reasons for access but also the possible effect of access on University values such as academic freedom and internal trust and confidence.

- System Protection, Maintenance, and Management

  University systems require ongoing maintenance and inspection to ensure that they are operating properly; to protect against threats such as attacks, malware, and viruses; and to protect the integrity and security of information. University systems also require regular management, for example, in order to implement new software or other facilities. To do this work, the University may scan or otherwise access user electronic information.

- Business Continuity

  User electronic information may be accessed for the purpose of ensuring continuity in business operations. This need can arise, for example, if an employee who typically has access to the files in question is unavailable due to illness or vacation.

- Safety Matters

  The University may access user electronic information to deal with exigent situations presenting threats to the safety of the campus or to the life, health, or safety of any person.

- Legal Process and Litigation

The University may access user electronic information in connection with threatened or pending litigation, and to respond to lawful demands for information in law enforcement investigations, other government investigations, and legal processes.

- Internal Investigations of Misconduct

The University may access user electronic information in connection with investigations of misconduct by members of the University community, but only when the authorizing person, after weighing the need for access with other University values, has determined that such investigation would advance a legitimate institutional purpose and that there is a sufficient basis for seeking such access. As described in Section VI of this policy, all decisions to access user electronic information are subject to review by an Oversight Committee.

This policy does not apply to reviews of research misconduct allegations conducted under established School-based policies.

II. Authorization of Access

Access to user electronic information should be authorized by an appropriate person, as set forth below. In deciding whether to approve access, the authorizing person should consider whether effective alternative means to obtain the information are reasonably and timely available. In all cases, access must comply with applicable legal requirements.

Authorization for access to user electronic information may be provided by the consent of the user.

Other cases should be handled as follows:

- If the user is a faculty member or other holder of an academic appointment at Harvard, the dean of the relevant Faculty must authorize access.
- If the user is an employee other than a faculty member: (1) the human resources officer or his/her designee for the relevant School or administrative unit must authorize access in business continuity cases; and (2) the dean of the relevant Faculty or the senior administrator of the relevant unit if not a Faculty, or their designees, must authorize access in investigative or other cases.
- If the user is a student, the School-level dean or the dean's designee must authorize access.

Any authorization of access shall apply only to the particular situation and user or users. Any other instance of access must be separately authorized.

No independent authorization is required for information technology personnel to conduct routine system protection, maintenance, or management purposes in accord with internal protocols and processes. Likewise, requests for access in connection with litigation, legal processes, or law enforcement investigations, or to preserve user electronic information for possible subsequent access in accordance with this policy, need no independent authorization if made by the Office of the General Counsel.

In exigent situations involving a threat to campus safety or the life, health, or safety of any person, access may be authorized by the Office of the General Counsel. If emergency conditions do not allow for prior authorization, the matter shall be reported to the Office of the General Counsel as promptly as possible.

For some requests to search user electronic data, it may not be possible to identify any particular user in advance. For example, requests for logs of access to a University facility (swipe card data) often are intended to find out who entered a facility during a particular period; in such cases, the requestor cannot identify a particular user or users because the goal of the search is to learn those identities. Such data requests may still be subject to one of the prior provisions of this Section II, for example, those relating to law enforcement investigations or emergencies. Otherwise, such data search requests must be authorized by the dean of the relevant Faculty or the senior administrator of the relevant unit if not a Faculty, or their designees, in the School or unit where the requestor works.

III. Notice

When the University intends to access user electronic information, notice ordinarily should be given to that user. All reasonable efforts should be made to give notice at the time of access or as soon thereafter as reasonably possible.

System protection, maintenance, and management — Individual notice is not required for ordinary system protection, maintenance, or management. Notice should be given if the access relates specifically to the activity of an individual user.

Business continuity — Individual notice is not required for access to user electronic information for purposes of business continuity, in accordance with established University practice and the common understanding that individual notice in such cases is typically not practical.

Legal restrictions — Individual notice is not required where the University is subject to legal constraints on its ability to give notice.

Emergencies and other extraordinary cases — Contemporaneous notice is not required in cases where there is insufficient time, where giving notice would otherwise interfere with an effective response to an emergency or other compelling need (e.g., at a stage of an internal investigation where giving notice may compromise the investigation), or where it is impractical (e.g., in the case of a former employee). The decision not to give contemporaneous notice must be made by the person designated by this policy to authorize the access. In such cases, notice will ordinarily be given as soon as practical.

The person designated by this policy to authorize access may decide not to give notice. Any such decision, and the reasons for it, shall be described in the records described in Part V of this policy and may be reviewed by the oversight committee, as set forth in Part VI.

IV. Scope of Access

The University shall adopt reasonable steps, whenever practicable, to limit access obtained under this policy to user electronic information that is related to the University's purpose in obtaining access. These steps will vary depending on the circumstances of the search and may include, by way of illustration, designing searches to find specifically designated items, as opposed to categories of information.

Participation in the search, and access to the information, should be limited to those personnel with a reasonable need to be involved.

V. Records of Process

Any person who authorizes access to user electronic information shall provide that reasonable records of the decision process and the reasons for the decision are made and preserved.

The persons who implement access to user electronic information shall make reasonable records and logs of the steps taken to access the information. All implementation records shall be delivered to and preserved by the University Chief Information Officer.

Copies of the information accessed should be retained as needed to effectuate the purposes of the access.

The accessed information and the records and logs of the search shall be kept appropriately secure.

In all instances of access under this policy, records adequate to permit effective review as described in Part VI of this policy should be kept.

VI. Oversight Committee

This policy, its implementation, and instances of access under this policy shall be subject to review by an oversight committee to be constituted by the University, which shall include faculty and senior administrators. The oversight committee shall make recommendations to the President as to the implementation of the policy and possible amendments. The oversight committee shall also make periodic public reports on the implementation of this policy.

In carrying out its responsibilities, the oversight committee may review the records described in Part V of this policy, subject to redaction as necessary to protect individual users.