Report of the Senate Working Group on IT Policy and Privacy

Respectfully submitted to the Senate Executive Committee for
further distribution to the entire University Community

March 20, 2018

1. Charge

The Senate Working Group on IT and Privacy Policy's primary task is to review the University Email Policy (http://tech.rochester.edu/policies/email-use-policy/) and University IT policy (http://tech.rochester.edu/policies/information-technology-policy/) and to recommend changes to these policies to strengthen the stated principles in the IT policy on Academic Freedom, Supportive Academic Environment, Accountability and Personal Use and Privacy. One consideration motivating this review is the search and distribution of faculty emails to faculty supervisors acknowledged by President Seligman in his statement of September 19 to the Faculty Senate. The committee will produce a report for the entire University community. The committee may additionally opt to produce a confidential report for senior administrators, Office of Counsel, the Faculty Senate Executive Committee and leaders of appropriate undergraduate and graduate student elected representative councils. The committee will select its own chair(s), who will be responsible for establishing, in consultation with the Office of Counsel representative, the requirements of confidentiality for members of the committee.

2. General Observations

In accordance with the charge, this report is meant to be distributed to the entire University community. This is no more than logical, since (i) the issues it deals with affect the entire community: undergraduate students, graduate students, administrative personnel, clinical personnel, faculty, outside advisory boards and even the Board of Trustees, as well as many departments and divisions with a wide range of processes and missions; and (ii) the issues it deals with are of great importance to the efficient and effective functioning of many parts of the University and of the University as a whole.

Formulating detailed policies that cover such a wide range of constituencies and their specific concerns is a task that falls beyond the resources and time available. Hence this report is limited to general considerations and recommendations. Specific details will need to be worked out by others. We hope, however, that this report will form the basis for a broad agreement on the principles that can guide the formulation of detailed policies for specific groups, areas and circumstances.

The core of our recommendations is a requirement to report searches of personal information to an independent committee with faculty and perhaps student and/or staff representation. We do not attempt to assess the appropriateness or legality of the email searches referred to in our charge. However, we do believe that these events have caused a significant deficit of trust in the University's ability to handle issues related to electronic records (and in particular email)

in an impartial manner. Assurances from University administrators alone cannot restore this trust. The only way to do this is through a requirement that (except when legal requirements dictate otherwise) all searches will be reported and reviewed by an independent body, and that the policies and processes that govern searches are faithfully followed. Hence our proposal for an independent Privacy Committee that reviews search requests, verifies that policies are being followed, and is consulted when policy changes are proposed.

3. Methodology

The committee examined policies from the following benchmark institutions:

Brandeis University	Emory University
Brown University	Georgia Institute of Technology
Boston University	Johns Hopkins University
Carnegie Mellon University	Massachusetts Institute of Technology
Columbia University	Northwestern University
Cornell University	University of Pennsylvania

The committee also examined three relevant policies at the University of Rochester:

University Email Policy (http://tech.rochester.edu/policies/email-use-policy/)
University IT Policy (http://tech.rochester.edu/policies/information-technology-policy/)
Acceptable Use Policy (https://tech.rochester.edu/policies/acceptable-use-policy/)

4. Findings

A. Most policies, including the University of Rochester's, explicitly mention academic freedom and right to privacy.

B. All policies, including the University of Rochester's, stipulate the institution's right to examine emails and other personal documents stored on or transmitted via institution owned equipment. There are several good reasons why the institution might need to examine email and other documents, including business continuity and complying with legal proceedings. As a consequence, many policies include mention that users should not expect their private emails to remain confidential.

C. Most policies stipulate who has the right to approve access to private files. Usually, the University Counsel has a prominent role in making approval decisions. Some limit the approval authority to just a few people, others delegate the approval authority to relatively many. The University of Rochester grants approval authority to President, Provost, Vice President of the University or Medical Center, Dean, CEO of Strong Memorial Hospital, Director of LLE or Director of MAG, and Vice Provost and Chief Information Officer, as well as the Vice President and General Counsel, more than most.

D. The University of Rochester's policies provide for more controls than most other universities regarding "Personal Communications". It specifies (i) processes to be followed for access requests; (ii) requires documentation of the reasons for a request for access; (iii) the Vice President and General Counsel is to be informed of all requests

and approvals or denials; (iv) notice to be given to users whose documents are accessed (with some exceptions); (v) specifies sanctions for violations of the policy. However see section 5A below.

E. What seems to be missing from most policies (including the University of Rochester's) is any kind of faculty involvement in deciding on granting access to personal records or reviewing the decisions made by administrators in this regard.

One university requires consultation with the Chair of the Faculty Senate before a search of personal records of a faculty member can be made, and a second requires all such searches to be reported within five days to an ombudsman selected by the Faculty Senate. To be clear, the results of searches are not shared with those consulted before the search or informed of the search afterwards, and in all cases policies require the conditions of court-ordered searches to be complied with.

5. Other observations regarding the University of Rochester's Policies

A. Having both an Email Policy and an Acceptable Use Policy appears redundant. Should these be combined?

B. The IT Policy states:

> "Personal Communications" are limited to faculty and student research, teaching, learning or personal (i.e. non-University related) emails, documents and correspondence. All other emails, documents, and correspondence prepared by a faculty member, student or employee in connection with his or her job responsibilities are defined as "University Communications" and may be accessed as needed for the purpose of carrying out University Business without seeking prior approval.

This would imply that, e.g., the internal communications of this committee, internal emails of the Faculty Senate Executive Committee, as well as most emails sent by staff, deans, vice presidents, provost and president could be accessed **without prior approval**. This seems to fly into the face of common sense.

C. Local policies are not dealt with in a clear manner. The University Email Policy very confusingly states "In the event such local policies or standards are inconsistent with this Policy, this Policy shall govern unless a more restrictive policy exists at the local level", while the Information Technology Policy states about the relationship between university and division or departmental IT policies: "In the event of inconsistency, the provisions of this Policy will prevail, unless the more specific policies are necessary to meet legal requirements governing certain types of information, in which case the more specific legal requirements and related policy will take precedence."

It would be far preferable to bring local policies into agreement with the global university policies, but at least the global policy should explicitly state that privacy protections in the global policy cannot be overridden by any local policy.

D. The policies are quite specific about how searches are to be conducted (see Information Technology Policy section II.II.B). We have not investigated how strictly these procedures are actually followed, but it might be worthwhile to investigate the feasibility of implementing access auditing systems for the various email systems employed by the University and possibly other systems. This might prevent unauthorized searches/access. In addition, we have not investigated the existence and disposition of archival copies of email, web searches, etc. The Policy on Retention of University Records seems to be outdated in this regard, since it still seems to assume that email and backups are stored on University owned.

6. Recommendations

A. Eliminate the distinction between "Personal Communications" and "University Communications" (see 4.B above). All communications as well as files on personal computers, browser data, and other personal data collected from networks should be treated as "personal" in the sense that they can only be searched after permission has been obtained, and any search must be reported and reviewed as described in part B below. All searches of electronic communications should be subject to common procedures addressing (i) who may initiate a request, (ii) what reasons for a search are permissible, (iii) who must be informed of the search, (iv) who must approve the search.

   Certain PCs and all institutional email accounts can be designated as "University Controlled", meaning their content is not considered personal and can be accessed without going through the approval process by persons already in possession of passwords, etc.

B. Searches of personal information should be a last resort. As much as possible, the information should first be requested from the person involved. Whenever circumstances permit, the person(s) involved should be notified of a search having been made as soon as possible. Exceptions to these principles may however be necessary due to specific circumstances.

C. Who has access to materials obtained from authorized searches, for what length of time and how the results of searches are distributed must be outlined in any search request, or documented with the search request as soon as a determination has been made. In principle, materials obtained must be destroyed as soon as possible, and access must be as restricted as possible to achieve the purpose of the search (once approved). If a search must be performed on the basis of a court order or other compelling outside legal requirement, the conditions imposed in such an order must generally be complied with.

D. Form a standing Privacy Committee charged with overseeing all University policies related to privacy, as well as oversight of the processes used to support these policies (e.g. it appears software is currently routinely installed on some user PCs that has the capability of searching the PC's hard disk and reporting the results to the IT department).

E. The Privacy Committee will consist of three or four tenured faculty members. The President, Provost, deans, associate deans and others of comparable rank will not be eligible to serve on this committee. Note that the committee will need some redundancy so that member(s) who have any type of (potential) involvement with a pending case can be recused. We propose that this committee include three members chosen by the Faculty Senate Executive Committee and that they serve staggered three year terms. Student and staff representation should be considered.

F. The Privacy Committee or two of its members will be informed of any access or search of personal information (emails, files, network data, etc.), if possible before the search, but in no case later than 2 business days after the search took place. Generally speaking, student and staff representatives should only be involved in cases involving students and staff respectively. The committee members will be expected to maintain the strictest confidentiality regarding search requests, and search results should generally not be shared with committee members.

G. The Privacy Committee should report to the Senate Executive Committee on at least an annual basis in general terms.

H. Any change to a policy related to privacy should be treated as a change to the faculty handbook: the Privacy Committee should be involved at an early stage and be asked to provide its recommendation on the policy change to the Faculty Senate, after which the Faculty Senate should have the opportunity to vote on the policy change.

I. Address observations 5.A and 5.C above

J. Consider reducing the number of individuals or roles that have approval authority (see Finding 3.C above).

K. Address the issues discussed in observation 4.D above.

L. It might be possible to tighten the procedures governing searches further. In any event it is important that all requested searches are routed through the University Counsel and the Privacy Committee so that a centralized record exists of search requests, searches executed and access and distribution rules established for every search requested or executed.

7. Working group members

Melissa Glasner, Graduate Student, Ovitt Lab, UR Medical Center
Harry Groenevelt, Associate Professor, Simon Business School, Chair
Carl Mueller, Professor, Department of Mathematics
Muthuramakrishnan Venkitasubramaniam, Associate Professor, Computer Science Department

The committee was assisted in its deliberations by:
Joe Doyle, Associate Counsel, Office of the Vice-President and University Counsel
Samantha Singhal, Co-Deputy CIO, Office of the CIO