User Electronic Information Access

Category: Operations; Students and Teaching
Approval: PVP
Responsibility: AVP-Information Technology
Date approved: September 12, 2016, October 11, 2016

Definitions:

"University systems" refers to all services, networks, and devices owned, provided, or administered by any department 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 Trent faculty, others holding academic appointments at Trent, students, staff, and other employees and anyone else authorized to access University Systems.

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

- Documents and communications, including 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;
- Information generated by automated processes triggered by that user's use of University systems, such as internet firewall records 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 Student Information System; or (b) information as described in (II), above, when accessed by the University without identifying or seeking to identify any particular user.

Purpose/Reason for Policy:

Members of the Trent 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, consistent 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 four 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 of the access.

Scope of this 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 Departments of the University.

This policy is inclusive of all user electronic information under the custody and control of the university. This information would generally relate to the current and historical operation and administration of the university, to students, applicants, alumni, staff, faculty, volunteers, researchers, and may include personal, academic, financial, curricular, clinical, and other information. Administrative records about research and scholarly activity, such as research grants held and publications generated are considered to be institutional records and are within the scope of this policy.

This policy does not apply to user electronic information not under the custody and control of the university, including:

- Research and study notes, teaching materials, reports, manuscripts, publications and communications of individual faculty, staff and students (unless specifically commissioned or prepared under contract for the University or prepared in the context of administrative work), or
- Information placed in the University Archives by or on behalf of a person or organization other than the University.

Policy Statement:

Reasons for Access:

The University does not 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.

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 intrusion, 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 needed files is unavailable due to illness or vacation.

Safety Matters

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

Legal Process or Litigation

The University may access user electronic information in connection with pending litigation, and to respond to lawful demands for information in law enforcement investigations, other government investigations, and legal processes. Additionally, the university may access user electronic information in response to FIPPA/access to information requests.

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.

Authorization of Access:

Access to user electronic information must 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 Trent, the Dean or Provost and Vice President Academic must authorize access in conformity with any relevant collective agreement.

- If the user is an employee other than a faculty member, then the department head must authorize access.
- If the user is a student, the Registrar, AVP Student Affairs, or the Provost and Vice President Academic must authorize access.
- Any authorization of access shall apply only to the particular situation. Any other instance of access must be separately authorized.

- In all cases above, the request will also be reviewed and approved by the Associate Vice President of IT. No independent authorization is required for information technology personnel to conduct routine system protection, maintenance, or management in accordance with internal protocols and processes. Information technology personnel have access to confidential information as a part of their job and may be bound by explicit or implicit expectations of privacy. Likewise, requests for access in connection with litigation, legal processes, or law enforcement investigations need no independent authorization if made by Risk Management, Human Resources or the Secretariat.
- In urgent situations involving a threat to campus safety or the life, health, or safety of any person, access may be authorized by Risk Management. If emergency conditions do not allow for prior authorization, the matter shall be reported to Risk Management 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. Information gained from such requests must be used only for the purpose underlying the request and shall not otherwise be recorded or used for other purposes.

Notice:

When the University intends to access user electronic information, notice, should be given to that user in advance if possible. When advance notice is not possible, reasonable efforts should be made to give notice at the time of access or as soon thereafter as possible.

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

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

Emergencies and other extraordinary cases: 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 notice must be made by the person designated by this policy to authorize the access.

Scope of Access:

The University shall adopt reasonable steps, whenever possible, 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 as determined by the individual granting access.

Contact Officer:

AVP, Information Technology

Date for Next Review:

September 12, 2018

Related Policies, Procedures & Guidelines

a) Computing Resources Acceptable Use Policy
b) Network Connection Policy
c) Computing Privileges Policy

Policies Superseded by This Policy:

a) Guidelines for Use of Information Technology