Access to User Electronic Information Policy

I. Policy Statement

Members of the WPI 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 WPI owns, provides, or administers. WPI makes these systems available for the purpose of carrying out WPI's various activities. WPI should be transparent about its policy regarding the circumstances in which it may access User Electronic Information stored in or transmitted through its systems, networks and devices. This policy therefore sets out guidelines and processes that apply when WPI seeks access to such electronic information, consonant with WPI'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 WPI; 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, as more fully set forth herein:

1. Access should occur only for a legitimate institutional purpose.
2. Access should be authorized by an appropriate and accountable person.
3. In general, notice should be given when User Electronic Information will be, or has been, accessed.
4. Access should be limited to the User Electronic Information required to accomplish the purpose.
5. Sufficient records should be kept to enable appropriate review of compliance with this policy.
6. Access should be subject to ongoing, independent oversight by a committee that includes representatives from the faculty and senior administration.

II. Scope

This policy sets forth guidelines and processes for WPI access to User Electronic Information stored in, or transmitted through, any WPI System. This policy applies to all units of WPI.

III. Definitions

"WPI Systems" refers to all services, networks, and devices owned, provided, or administered by any unit of WPI, 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. "WPI Systems" does not include User-owned devices.

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

"Authorizer" refers to the individual tasked with granting or denying access to User Electronic Information.

"Legitimate Institutional Purpose" refers to a reason WPI may access User Electronic Information, as set forth in this policy.

"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 WPI Systems, such as tracks of internet use and logs of access to facilities.

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

IV. Policy

A. Access for Legitimate Institutional Purposes

WPI does not routinely monitor the content of information transmitted through, or stored in, WPI Systems. WPI may obtain access to User Electronic Information for a Legitimate Institutional Purpose as set forth in this policy. The paragraphs below describe certain purposes for which WPI may access such User Electronic Information. While this list is expected to cover most instances of access, the list is not intended to be exhaustive. WPI may access User Electronic Information for comparable reasons that likewise advance a Legitimate Institutional Purpose, as determined by an Authorizer, pursuant to this policy and subject to review by the oversight committee as described in Part IV(F).

Although this policy applies to the User Electronic Information of faculty, staff, and students alike, in evaluating the reason for access, the Authorizer should in each case weigh not only the stated reasons for access but also the possible effect of access on WPI values such as academic freedom and internal trust and confidence.

1. System Protection, Maintenance, and Management

WPI 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. WPI Systems also require regular management, for example, in order to implement new software or other facilities. To do this work, WPI may scan or otherwise access User Electronic Information.

2. Business Continuity

User Electronic Information may be accessed for the purpose of ensuring continuity in business operations. This need may arise, for example, if an employee who typically has access to the files in question is unavailable due to illness, termination, or other prolonged absence where the User is unavailable. This exception shall not be used to obtain intellectual property that is solely owned by the User (e.g., faculty course materials).

3. Safety Matters

WPI 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.

4. Legal Process and Litigation

WPI 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.

5. Internal Investigations of Misconduct

WPI may access User Electronic Information in connection with investigations of misconduct by members of the WPI community, but only when the Authorizer, after weighing the need for access with other WPI 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 IV(F) 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 WPI policies.

B. Authorization of Access

In deciding whether to approve access, the Authorizer should consider whether effective alternative means to obtain the information are reasonably and timely available. In all cases, access must comply with all applicable legal requirements.

Any authorization of access shall apply only to the particular situation and User(s). Any other instance of access must be separately authorized.

For some requests to search User Electronic Information, it may be impossible to identify any particular user in advance. For example, requests for logs of access to a WPI facility (e.g., 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(s) because the goal of the search is to learn those identities. Regardless, such data requests may still be subject to one of the Legitimate Institutional Purposes set forth in Section A.

Authorization for access to User Electronic Information may always be provided by the consent of the User. Authorizers for all other cases are summarized in the following chart:

	Legitimate Institutional Purpose				
User	**System Protection, Maintenance & Management**	**Business Continuity**	**Safety Matters[1]**	**Legal Process and Litigation[2]**	**Internal Investigations and Misconduct**
Faculty Employee	Information Technology	Dean of department	Office of the General Counsel	Office of the General Counsel	Dean of department
Non-Faculty Employee	Information Technology	VP for Talent & Inclusion	Office of the General Counsel	Office of the General Counsel	Senior Administrator of relevant unit
Student	Information Technology	VP of Student Affairs	Office of the General Counsel	Office of the General Counsel	VP of Student Affairs

Notes:
1. 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.
2. This category includes preservation of User Electronic Information for possible subsequent access in accordance with this policy.

C. Notice

When WPI 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 WPI practice and the common understanding that individual notice in such cases is typically not practical.

- Legal restrictions. Individual notice is not required where WPI is subject to legal constraints on its ability to provide notice.

- Emergencies and other extraordinary cases. Contemporaneous notice is not required in cases where there is insufficient time, where providing 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 provide contemporaneous notice must be made by the Authorizer. In such cases, notice will ordinarily be provided as soon as practical.

D. Scope of Access

WPI shall adopt reasonable steps, whenever practicable, to limit access obtained under this policy to User Electronic Information that is related to WPI's Legitimate Institutional Purpose. 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.

E. Records of Process

Authorizers shall provide and preserve reasonable records of:

1. Their decision to grant or deny access to User Electronic Information, including their process and reasons for making such a decision; and
2. If access is granted to User Electronic Information, records of the steps taken to access the User Electronic Information.

The Authorizer shall deliver those records to WPI's Chief Information Officer for preservation in a manner sufficient to permit effective review as described in Part F of this section. The accessed User Electronic Information and the records of the access shall be kept appropriately secure. Copies of any accessed User Electronic Information may be retained as needed to effectuate the purposes of the access.

F. 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 WPI, which shall include faculty and senior administrators. The Oversight Committee shall make recommendations to the Administrative Policy Group as to the implementation of this 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 E of this policy, subject to redaction as necessary to protect individual Users.

V. Questions

For questions about this policy, please send an email to its@wpi.edu or OGC@wpi.edu.

* * *

Policy Sponsors: Chief Information Officer, Provost, General Counsel
Responsible Departments: Information Technology, Academic Affairs, Office of the General Counsel
Effective Date (i.e., date of Presidential Approval): September 18, 2020
Revision Date: N/A