University of Pittsburgh
Access to and Use of University Computing Resources
AO 10

Implementing Executive:	Vice Chancellor and Chief Information Officer
Responsible Unit:	Pitt Information Technology
Category:	Administration and Operations
Effective Date:	March 5, 2024

I. Purpose

This policy defines and governs what is acceptable access and use of computing resources owned, leased to, or contracted by the University of Pittsburgh.

II. Scope

This policy governs who may access and use computing resources provided by the University. While the University's computing environment is in a constant state of change, it consists generally of Applications and Services, communications systems, and Data Storage whether the systems and End User Devices are owned or leased by the University or provided by third-party vendors under contract to the University.

Personally owned and third-party End User Devices, applications, and services are outside the scope of this Policy, even when those items access the University Network's (PittNet) to access a third party application or service. Accordingly, the University's response to requests for access to traffic on PittNet between Personal Computing Resources and third-party applications and services is outside the scope of this Policy.

III. Definitions

A. University Computing Resource – any computing device, system, or application provided by the University. Such resources include, but are not limited to:

- Applications and Services: enterprise systems such as the learning management system, student and financial systems, HR and payroll systems, as well as departmental Applications and Services.
- Data Storage: systems and devices used for the storage and retrieval of institutional, research, and in some cases, personal files and other electronic records.
- End User Devices: personal computers, laptops, tablets, and other devices owned by the University and assigned to students, faculty, or staff employees.

B. Data: the actual contents of files and electronic communications sent across the University Network and/or stored on University Computing Resources or third party computing resources.

C. Metadata: descriptive information about Data, including but not limited to the time sent or stored, origin, destination, sender, recipient. Metadata does not reveal the contents of the actual Data.

D. PittNet - the data communications network operated by the University to provide access to University Computing Resources. See Policy AO 38 – University Network for further information on PittNet.

E. Personal Computing Resource – any device or computing resource privately owned which can be connected to PittNet and/or used to access other University Computing Resources. Such End User Devices include, but are not limited to laptop and desktop computers, "smart phones," and tablets.

F. Personal Data – any and all messages, saved or stored passwords, and electronic files of any kind belonging to a particular user.

G. University Computing Account – an account granted to and used by a University Community Member that permits access to any or all University Computing Resources and PittNet.

H. University Community Members – students, faculty, staff, contractors, guests, and any members of the general public granted permission to access and use University Computing Resources.

IV. Policy

University Community Members generally use University Computing Resources when performing their employment, learning, teaching, research, providing or receiving community services, or when conducting University business. The use of University Computing Resources and PittNet is to be conducted without creating excessive demands that interfere with the activities of other users. Normal use is unlikely to violate this provision, but users who know that their legitimate activities could produce very heavy demand on University Computing Resources should consult with Pitt Information Technology (Pitt IT) at (412) 624-HELP (4357) for assistance before beginning such activities.

A. Prohibited Activity

University Computing Resources and PittNet may not be used for:

- Performing an action that is in violation of any University Policy, including the requirements described in RI 01, Conflict of Interest for Research; CS 10, Participation in Political Campaigns;[1] and CS 07 Nondiscrimination, Equal Opportunity, and Affirmative Action;

- Performing any activity prohibited by law, including illegal file sharing or theft of intellectual property;
- Abusing or misusing University Computing Resources or PittNet in such a way as to cause damage or system interruptions; or
- Borrowing, lending, falsifying, or "hacking" into a University Computing Account or allowing or facilitating unauthorized access to University Computing Resources by a third party.

B. Resource Security

Any user of University Computing Resources and PittNet must follow all University computer security standards regardless of whether the user's device is provided by the University or is personally owned. Additionally, all users must provide best efforts to ensure that their University-provided or personally-owned End User Devices are free from viruses and malicious software before accessing University Computing Resources or making connections to PittNet. Current device security standards are available on Pitt IT's website and include topics such as installation and maintenance of operating system and other security patches and updates, encryption of sensitive information, reporting loss or theft of equipment, and other measures.

When using University Computing Resources while based outside the United States, the user must follow additional security procedures. It is recommended that faculty and staff utilize loaner equipment intended for travel abroad in place of End User Devices normally used at home. These security procedures are available at https://globaloperations.pitt.edu/traveling-abroad/technology/.

Departments must ensure that all Personal Data is permanently erased from University-owned End User Devices used by former University Community Members before reassigning those End User Devices to others. Departments no longer planning to use such devices must work with Pitt Surplus Property to arrange for the proper disposal of such equipment.

C. User Expectations of Privacy

In the normal course of events, Data transferred across PittNet and stored on University Computing Resources is not subject to surveillance by the University. As the owner of University Computing Resources, however, the University may need to or be legally required to access information stored on those Resources. In addition, the University may make use of Metadata for analytical, capacity planning, and other similar purposes. Accordingly, users of University Computing Resources and PittNet should be aware that under certain limited circumstances, the University may access or provide others with access to any Data, including

[1] Please visit Frequently Asked Questions: Political Activity at the University for information on permissible political activity on campus.

Personal Data, stored on its systems. Situations that may require access to this information, include, but are not limited to:

- Compliance with other University Policies;
- When a user has separated from the University, dies, or becomes incapacitated;
- In response to a subpoena, court order, or search warrant for an ongoing or pending criminal investigation or civil action;
- In response to a copyright infringement claim or similar complaint received by the University based on alleged improper access to or excessive downloads of third party copyrighted materials;
- When necessary for maintaining and troubleshooting problems with University Computing Resources and PittNet;
- In conjunction with ongoing security assessments conducted by or through the Pitt IT Information Security Department; or
- In conjunction with research integrity assessments and investigations, as stipulated in Policy RI-07, Research Integrity.

In all such cases, the Data accessed will be used solely for the approved purpose.

Pitt IT refers requests for access to information traveling across PittNet to the appropriate service provider (unit or school within the University or a third party) where the information is actually stored.

V. Noncompliance

University Community Members who do not comply with this Policy may be subject to disciplinary action in accordance with the University's disciplinary guidelines, including, but not limited to, loss of access.

VI. Governance or Responsibilities

User Responsibilities

- Comply with all federal, state, and other applicable laws, as well as University policies and procedures, that are relevant to accessing and using University Computing Resources.
- Use University Computing Resources and PittNet only in the manner and to the extent authorized. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.
- Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected.

- Respect the finite capacity of University Computing Resources and limit their use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users.

Pitt IT Responsibilities

- Establish and maintain, working with appropriate stakeholder units, access controls and user permissions to help ensure that only properly authorized users gain access to University Computing Resources.
- Establish, maintain, and communicate acceptable use standards as needed for University Computing Resources and PittNet.

VII. Contact Information

This Policy is posted under Administration & Operations Policies on the Office of Policy Development & Management's website and can be found at: https://www.policy.pitt.edu/.

For specific questions related to this Policy, please contact Pitt IT at: https://www.technology.pitt.edu/about-us/contact-us.

VIII. Related Authorities and Policies

- Pitt IT Policies and Procedures:
  - Acceptable Use of PittNet and University Enterprise Applications and Services
  - ResNet Acceptable Use Policy
- Pitt Global Operations Technology website
- University Political Activity FAQ