

# Pratt Institute Computer and Network Responsible Use Policy

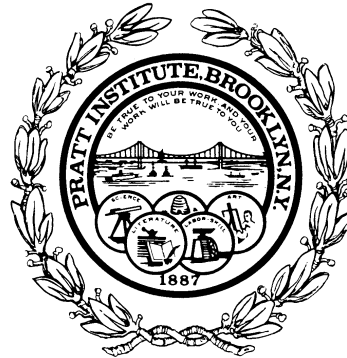
---

Revision 9

Policy governing all Computer and Network  
Use for Pratt Institute

First Approval: June 1998.

Contact Academic Computing concerning the  
status of this document: [ac@pratt.edu](mailto:ac@pratt.edu)  
718-636-3603



**Contents**

Policy Information ..... 3  
    Policy Statement ..... 3  
    Reason for Policy ..... 3  
    Affected Entities ..... 3  
    Related Documents ..... 3  
    Distribution ..... 3  
    Contacts ..... 4  
Overview ..... 5  
    Mission ..... 5  
    Description of the Pratt Network ..... 5  
User and System Administrator Responsibilities ..... 6  
    Individual's Responsibilities ..... 6  
    System Administrator's Responsibilities ..... 6  
Procedures ..... 7  
    Institute Standard Procedures ..... 7  
    Policy Violations ..... 7  
    Reporting Violations ..... 8  
    Procedures for Handling Violations ..... 8  
    Consequences of Violations ..... 8  
    Web Page Standards ..... 8  
Employee Policy ..... 9  
    Overview ..... 9  
    Limited Activities ..... 9  
    Prohibited Activities ..... 9  
    Procedures for Handling Violations ..... 10  
    Consequences of Violations ..... 10  
Pratt Universal E-mail System ..... 11  
    Definition ..... 11  
    Purpose ..... 11  
    Message Protocol ..... 11  
    Message Review and Approval Process ..... 12  
    Message Archiving ..... 12  
Server Accounts and Internet Access Eligibility ..... 13  
    Eligibility Categories ..... 13  
    Obtaining an Account ..... 13  
Laptop Administrative Access Policy ..... 14  
    Introduction ..... 14  
    Policy ..... 14  
    Procedure ..... 14  
    Policy Guidelines ..... 14  
    Revocation of Administrative Rights ..... 15

## **Policy Information**

### ***Policy Statement***

---

All members of the Pratt community are expected to use its computer and network resources in a responsible manner. In the event of violations of institutional policies or codes, or of state or federal laws, use of Pratt computers or networks may be restricted. Specifically, Pratt Institute reserves the right to limit access to its networks or Institute computers and to remove or limit access to material contained in its computers.

### ***Reason for Policy***

---

- To protect the Institute against damaging or legal consequences.
- To enforce its policies regarding harassment and the safety of individuals.
- To prevent the posting of illegal software and other copyrighted materials.
- To secure the integrity of computers, networks and data, both Institute-owned and reachable through the Internet.
- To ensure that the rules governing computer and network use comply with and support other Institute rules and codes of conduct.

### ***Affected Entities***

---

All members of the Pratt community, specifically any persons accessing computer or network resources through any Institute facility or through the network or dial-in facilities.

### ***Related Documents***

---

- Pratt Institute Student Handbook
- Pratt Institute Internet User's Guide

### ***Distribution***

---

All members of the Pratt Institute community.

### ***Contacts***

---

Call or e-mail these offices if you have questions regarding the following areas:

- Policy Issues

Student Life ..... stulife@pratt.edu .....718-636-3711

Academic Computing ..... ac@pratt.edu .....718-636-3603

- Computers and Networks

Academic Computing ..... ac@pratt.edu .....718-636-3603

Internet Systems Administration ..... sysadmin@pratt.edu .....718-636-3603

Network Security ..... cert@pratt.edu .....718-636-3765

- Health or Safety

Pratt Security ..... security@pratt.edu .....718-636-3540

## Overview

### *Mission*

---

Pratt Institute's mission is to educate men and women to become creative, responsible professionals who will contribute fully to society. The Institute upholds values and standards that support that mission and holds high expectations regarding the conduct of students, faculty, and staff. Above all, we respect one another and behave in ways that advance the free association of people and ideas. We cherish the diversity represented by our people, their disparate values and ideas; while, at the same time, we expect one another to value and uphold the community standards essential to the pursuit of academic excellence and social responsibility. The Board of Trustees reinforced these ideals by passing a resolution on freedom of expression in 1992:

"It is resolved that: Pratt Institute supports and upholds freedom of speech and other forms of expression because these freedoms are essential to (our educational mission). At the same time, Pratt recognizes that such freedoms exist in the context of law and responsibility for one's actions and, therefore, the exercise of these rights must not deny the same rights of others."

Such is the spirit in which the Computer and Network Responsible Use Policy is written. Access to the Institute's network and other computer resources is not a right but a privilege, and the Institute takes seriously its obligation to protect itself and its members against the misuse of the network and other computer resources as well as from liabilities that might be imposed against it and its members by such misuse. Therefore, the Institute reserves the rights to not only extend but also to limit or restrict computing privileges and access to its computer resources. All users are expected to know, understand and abide by the regulations set forth in this Statement.

### *Description of the Pratt Network*

---

Pratt provides network access through its data cabling plant to all dormitory rooms, administrative offices and computer labs. In addition, network access is available in the offices and computer classrooms at Pratt Manhattan and by wireless access.

Pratt (pratt.edu) is a registered, directly connected domain on the Internet, gaining access via Lightpath, our up-stream provider. As a result, all Pratt computers connected to the local network, whether Institute or privately owned, share equally in the benefits and responsibilities of our greater Internet connectivity.

---

## User and System Administrator Responsibilities

### *Individual's Responsibilities*

---

- Creating, securing and remembering individual passwords
- Adhering to quotas and file size restrictions on shared systems and processes
- The backup and safekeeping of all data files
- Obeying Institute policies and state and federal laws
- Recognizing that user activity reflects on both the individual and Pratt Institute
- Protecting other's privacy as well as one's own.

### *System Administrator's Responsibilities*

---

- Performing periodic security surveys to ensure that shared systems are protected to reasonable degree
- Treat all user files as private and confidential
- Obtaining written permission from an officer of the Institute prior to examining any user files
- Obtaining written permission from an officer of the Institute prior to restricting or disabling any user account
- Perform maintenance as necessary to help ensure uninterrupted service
- Performing scheduled backups of shared systems but without specific responsibility for the integrity of the data housed on those systems
- Perform the technical enforcement of this policy in cooperation with the appropriate authorities
- Ensure that all user accounts meet Pratt eligibility requirements

## Procedures

### *Institute Standard Procedures*

---

Pratt Institute does not monitor the content on or generally restrict access to its computers or networks, including privately owned computers in dormitory locations. However, Pratt reserves the right to monitor activity within its domain and to limit or deny access to Institute-owned computers and networks in the following instances:

- When network activity is reported which violates Institute policies, or state or federal laws.
- When a report is received that materials are posted on Pratt owned computers, or computers inside the Pratt domain, which violate Institute policies, or state or federal laws.
- When an incidence is reported of the commercial use of Pratt owed computers, or computers inside the Pratt domain, if the commercial activity uses Pratt's network services.

### *Policy Violations*

---

Violations of this policy may include using Pratt Institute computers or networks to:

- Harass, threaten, libel or slander or otherwise cause harm to specific individuals or classes of individuals whether by direct or indirect means.
- Cause destruction or damage to equipment, software, or data belonging to the Institute or to others.
- Disrupt or impair the activities of others including the unauthorized monitoring of electronic communications.
- Copy, download or transmit across Pratt's network, illegal, proprietary, or unauthorized copyright-protected material.
- Use of the Institutes' trademarks, logos, or copyrights without prior approval.
- Develop programs or use existing programs that harass other users; infiltrates a computer or computing system; damages or alters software components of a computer or computing system; or introduces computer viruses.
- Gain unauthorized access to other systems, facilities or data either directly or via the network.
- Tamper with others' files, storage media, passwords, accounts; or represent others when sending messages or engaging in conferences.
- Conduct any commercial activity, including any activity published from personally owned computers and/or personal web pages, but which use the Pratt network. This includes using e-mail to solicit sales or conduct business, setting up a web page to advertise or sell a service, or posting an advertisement to a News group.
- Excess personal use of e-mail that interferes with other users or services by burdening Pratt's network or systems or which attacks outside domains. Abuse includes, but is not limited to, spamming, chain letters, letter bombs or any other type of widespread distribution of unsolicited e-mail.

- Violate any state or federal law.

---

### ***Reporting Violations***

---

Violation reports will be accepted from both within the Pratt domain and externally. The targeted individual or representatives of targeted groups should report violations but any violation report will be considered. In the event that you believe that a violation of this policy has occurred, contact Academic Computing or the Office of Residential Life. In addition, contact Pratt Security if you believe that an individual's health or safety may be in jeopardy.

---

### ***Procedures for Handling Violations***

---

In case of a written, oral or electronically transmitted complaint of misuse of this policy, the Director of Academic Computing or designee will request authorization to access information contained in that user's account and, if warranted, to suspend the account until the matter is resolved.

Access to and suspension of accounts must be recorded and the alleged offender(s) notified as soon as possible. If the complaint appears to have merit, the Vice President of Student Life and Director of Academic Computing will meet with the alleged offender, and will follow the Institute's judicial procedural guidelines.

---

### ***Consequences of Violations***

---

Pratt Institute reserves the right to monitor, restrict or deny access to its computers and networks in the event of a violation of this policy, other Institute policies, or of state and federal law. As stated above, penalties will be in accordance with Institute guidelines. However, Pratt will cooperate with outside law enforcement agencies in the investigation of criminal activity occurring within the Pratt domain.

---

### ***Web Page Standards***

---

All World Wide Web home pages that represent the Institute or any of its departments or organizations are required to adhere to the following standards:

- Provide at least one link between organizational home pages and the Institute's home page ([www.pratt.edu](http://www.pratt.edu)).
- Secure the approval of Institutional Advancement to use the Pratt Institute logo.
- Display full and accurate description of a department or service when publishing via the Institute home page (such descriptions may be obtained from the Bulletin, the Student Handbook, etc.)
- Ensure that the home page contains a contact e-mail address and a last modified time stamp.
- Maintain home page information in an up-to-date and accurate fashion.
- Ensure that information contained in the home page is of highest editorial standards (spelling, punctuation, grammar, style, etc.).
- Ensure that the Pratt Institute Web Page documents contain officially recognized names of departments and titles of personnel.



## Employee Policy

Pratt Institute employees are covered by all other sections of the Computer and Network Responsible Use Policy. In addition, the following sections apply specifically to employees.

### *Overview*

---

Computing resources provided by Pratt Institute to employees are intended to be used for Institute business and educational purposes only. Pratt encourages the use of the Internet and e-mail because they can make communications more efficient and effective. However, all computing resources, including Internet service and the contents of e-mail remain Pratt property.

Every employee has a responsibility to maintain and enhance the Institute's public image and to use e-mail and access to the Internet in a productive manner. To ensure that all employees are fully aware of these responsibilities, the following guidelines have been established. Any improper use of the Internet, e-mail, or other Institute-owned computing resources is unacceptable and will not be permitted.

### *Limited Activities*

---

- Computing systems may not be used to play computer games during work periods.
- Limited personal use of computing resources is allowed at the supervisor's discretion, following the example set of allowing limited personal telephone calls and storage of personal property.
- Pratt cannot guarantee the privacy or confidentiality of e-mail, electronic documents, or other materials transmitted via the network. Any messages that are confidential as a matter of law should not be communicated via e-mail.

### *Prohibited Activities*

---

- Use of electronic media for any other purpose that is illegal or against Institute policy or contrary to the Institute's best interest.
- Solicitation of non-Institute business or any use of the company e-mail or Internet services for personal gain.
- Use of non-public institutional information for personal ends, or obstructing its use for proper institutional operation.
- Use of institutional computing facilities to effect or receive the electronic transfer of funds for purposes unrelated to Institute business purposes.
- Use of the network or e-mail in a manner that is disruptive to the work or educational environment. Employee policies which cover the display or transmission of offensive or disruptive materials remain in effect when applied to network and computer use.
- Use of Institute resources for transmitting, retrieving, or storage of any files or communications of a discriminatory or harassing nature or materials that are obscene.

- Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual's race, age, gender, disability, religion, national origin, physical attributes or sexual preference shall be transmitted. No abusive, profane or offensive language is to be transmitted through the Institute's e-mail or Internet system.
- Mass e-mail is limited to items that are genuinely essential to the entire Pratt Institute Internet population, such as messages covering security issues or system outages. Announcements of events, special programs and all other mass e-mail messages are to be disseminated according to the Universal E-Mail System.

### ***Procedures for Handling Violations***

---

In case of a written, oral or electronically transmitted complaint of misuse of this policy, the Director of Academic Computing or designee will request authorization to access information contained in that user's account and, if warranted, to suspend the account until the matter is resolved.

Access to and suspension of accounts must be recorded and the alleged offender(s) notified as soon as possible. If the complaint appears to have merit, the Directors of Human Resources and Academic Computing will meet with the alleged offender, and will follow the Institute's judicial procedural guidelines.

### ***Consequences of Violations***

---

Pratt Institute reserves the right to monitor, restrict or deny access to its computers and networks in the event of a violation of this policy, other Institute policies, or of state and federal law. As stated above, penalties will be in accordance with Institute guidelines and in the case of employees may include termination. In addition, Pratt will cooperate with outside law enforcement agencies in the investigation of criminal activity occurring within the Pratt Internet domain.

## Pratt Universal E-mail System

### *Definition*

---

The Pratt Universal E-mail system is defined as the collection of individual email addresses with a pratt.edu suffix that have been assigned by Pratt administration to faculty, students, and staff for use in conducting official institute business. Email lists developed by various divisions or units within the institute for their specific uses are not considered part of Pratt's Universal E-mail system.

### *Purpose*

---

The Pratt Universal Email system is intended to be used only for official and essential Institute-wide business that applies to large groups of constituents: including students, faculty, and staff. The Universal E-mail system does not provide access to email lists to any group at Pratt, but serves as an "electronic mailing service" for approved official communications. Every effort must be made to clearly identify the specific desired recipient group in order to prevent unwanted "spamming".

This policy is not intended to apply to normal and ongoing communications between matriculated students and the Office of the Registrar. All messages must conform to Pratt's "Network Use Policy".

### *Message Protocol*

---

- Message should be brief, concise, and clearly identify the intended recipients.
- Subject line must contain a description of the subject of the message.
- Embedded images, logos, etc. shall not be used.
- Attachments will generally not be allowed. Information should be contained in the body copy.
- If additional documents are required, documents should be posted on an appropriate website with a hot-link to the site included in the body text.
- All messages will be sent from one of two source email addresses to allow for filtering at the receiver's option. The decision about the source email address shall rest with the Director of Academic Computing.
  - alert@pratt.edu will be used as source for critical messages pertaining to the health, safety, and welfare of the community.
  - announce@pratt.edu will be used for all other approved messages.
- All messages must contain a hot-link to the originator's email address to allow recipients to follow up with questions or comments.
- Distribution of repeat messages or reminders is allowed only for alerts since repeat announcement messages will be interpreted as spamming.

---

### *Message Review and Approval Process*

---

- The entire copy for the message, along with the intended recipient group, must be submitted to the head of the division requesting the communication (President, Vice-President, or Provost)
- Division heads shall review for approval all requests within that division.
- Decisions on appropriateness and content shall remain solely the discretion of the Division Head. Editorial assistance is suggested from the Office of Communications (ext. 4515) to insure appropriate use of language.
- Upon approval for posting by the Division Head, the message with approval must be submitted to the Director of Academic Computing (envoy@pratt.edu) in electronic form.
- The Director of Academic Computing will manage transmission of the message including appropriate database, coordination with our Datatel systems, and transmission scheduling and timing. Every attempt will be made to provide transmission of approved messages with three business days of final submission.
- Copies of each communication will also be sent to the appropriate division head and the originating staff member as transmission confirmation.

---

### *Message Archiving*

---

- The Director of Academic Computing will maintain record files containing a copy of all approved and transmitted messages, including description of recipient group.
- This information shall be reported to Senior Staff on a quarterly basis to allow for review and policy adjustments as may be appropriate

---

## Server Accounts and Internet Access Eligibility

Pratt Institute encourages communication among all members of the campus community. It also recognizes the increasing need for this community to access the valuable resources found on the Internet. However, Pratt must manage its resources in an effective and equitable manner and must provide network security. This section identifies eligibility categories for members of the Pratt community for accounts on local servers and for access to the Internet whether directly through campus or departmental servers or through modems or other dial-up devices.

As a result of limited bandwidth, and to preserve a secure computing environment, all other persons and organizations not included in these categories are ineligible for server accounts and Internet access. Ineligible accounts and the servers which host ineligible accounts or provide ineligible access will be summarily disabled or blocked.

### *Eligibility Categories*

---

#### **Faculty**

Regular full and part-time Pratt faculty, as defined and listed by Human Resources, are eligible for Pratt server accounts and Internet access.

#### **Administrators and Staff**

All full and part-time staff, as listed by Human Resources, are eligible for server accounts and Internet access. However, Internet access from the workplace is authorized only with departmental permission.

#### **Students**

Matriculated Pratt students who possess a validated Student Identification Card and are enrolled for regular credit classes are eligible for Pratt server accounts and Internet access.

Other students in programs sponsored by units not in the above category may be given server accounts and access to the Internet with the permission of their sponsoring units (e.g., School of Professional Studies). The sponsoring unit must certify that these individuals are students actively enrolled in one of their programs for the current term and are eligible for Internet access.

#### **Alumni**

Pratt alumni who have a valid Alumni Activity Card may obtain a server account and Internet access from Pratt. The Activity Card, available from Institutional Advancement, must be renewed in order for the account to be maintained.

### *Obtaining an Account*

---

All Internet accounts and Internet access for Pratt Institute faculty, staff, and students are provided at no cost to the individual and are automatically created.

## Laptop Administrative Access Policy

### *Introduction*

---

The Administrative Access Policy defines under what circumstances and to what extent administrative access rights are granted to non-support personnel so that they can successfully perform their Pratt-related computing activities. Pratt is committed to providing reliable technology in a stable computing environment while maintaining data security and preventing the violation of software copyright laws; this policy supports that commitment.

The granting of enhanced access rights will be in accordance with all other sections of this policy, specifically: "Pratt reserves the right to limit access to its networks or computers in the event of violations of institutional policies or codes, or of state or federal laws."

### *Policy*

---

By default, users of Pratt-owned laptops have standard user-access levels which provide the ability to create, edit or delete any end-user data as well as a limited amount of interface customization such as creating shortcuts and changing the look of the display. This policy will establish exemptions to the default settings and may permit an end-user to install software, printers and other peripherals.

It will also provide users the ability to change security settings, alter user accounts, change file-level permissions and modify the operating system. Any of these activities may make the computer unstable or damage the operating system.

These exemptions may be granted to faculty and staff members who require an administrative level of access on a Pratt-owned laptop to perform job-related tasks.

### *Procedure*

---

Written justification is required to grant administrative access rights. Requests must contain an explanation including specific job-related or academic tasks that aren't possible to achieve without administrative access. The requests should be sent via email to the Service Desk at [services@pratt.edu](mailto:services@pratt.edu). The request will then need to be reviewed and approved by the requester's division head before implementation.

### *Policy Guidelines*

---

- All laptops covered under this policy are Pratt property and are intended for Institute business or academic use.
- Only software and peripherals related to Pratt business and academic activities will be installed.
- No software that alters the base operating system or exposes the computer to viruses, worms or other malware will be installed.
- No software will be installed that uses excessive network resources or adversely affects any other computer.

- No software will be installed that establishes network shares which either result in an increase in bandwidth utilization or has the potential to create security problems.
- No software will be downloaded or installed which is illegal or violates copyright.
- Any commercial software, other than those included in the default Pratt configuration, must have appropriate licensing documentation. Software in this category will not be supported by the Pratt Service Desk and will be removed during normal repair processes if necessary to restore system functionality.
- Full administrative and remote access will be preserved for the IT Service Desk.
- For security purposes, the software-based tracking system Computrace and Sophos Anti-Virus will be preserved.
- All laptops will be configured to use Pratt's Active Directory domain.
- At least once every six-months all systems covered under this policy will be attached to the Pratt network to be registered through network services and have anti-virus software updated.

### ***Revocation of Administrative Rights***

---

Repeated occurrences of problems with the operating system or system security or any activities that violate this policy may result in the revocation of administrator level access.