



# *RESPONSIBLE USE OF COMPUTER NETWORK RESOURCES*

# RESPONSIBLE USE OF COMPUTER NETWORK RESOURCES

## PRATT'S POLICY ON COMPUTER AND NETWORK RESOURCES

Pratt's policy on computer and network resources is intended to:

- Protect the Institute against legal or other negative consequences
- Prevent the posting of illegal software and other copyrighted materials
- Secure the integrity of its computers, networks and data, and those with approved access to its network
- Ensure that the rules governing computer and network use comply with and support other Institute rules and codes of conduct

## WHAT IS THE POLICY AND HOW DOES IT AFFECT ME?

All members of the Pratt community are expected to use Pratt's computer and network resources in a responsible manner. The Institute's policies are clear as to the consequences of misuse of these resources.

In the event of violations of institutional policies or codes, or of state or federal laws, the Institute reserves the right to limit or restrict computing privileges and access to its computer resources and stored data.

All users are expected to understand and abide by the regulations set forth in this pamphlet as a condition for receiving an authorized account with the Institute.

## WHO IS AFFECTED BY THIS POLICY?

This policy applies to any member of the Pratt community who accesses computer or network resources through any Institute facility or through the network.

## WHAT DO YOU MEAN BY THE PRATT NETWORK?

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

All Pratt computer users connected to the network share equally in the benefits and responsibilities of our greater Internet connectivity.

## YOUR RESPONSIBILITIES AS A PRATT SYSTEM USER

As a user of Pratt's computer resources you are responsible for the following:

- Creating, securing, and remembering individual passwords
- Adhering to quotas and file size restrictions on shared systems and processes
- Backing up and safekeeping of all data files
- Obeying Institute policies and state and federal laws
- Recognizing that user activity reflects on both the individual and the Institute
- Respecting and protecting other's privacy as well as your own

## YOUR RESPONSIBILITIES AS A PRATT SYSTEM ADMINISTRATOR

As a Pratt system administrator you are responsible for the following:

- Performing periodic security surveys to ensure that shared systems are protected to a reasonable degree
- Treating all users' files as private and confidential
- Obtaining written permission from a designated officer of the Institute prior to examining any user files
- Obtaining written permission from a designated officer of the Institute prior to restricting or disabling any user account
- Performing maintenance as necessary to help ensure uninterrupted service
- Executing the technical enforcement of this policy in cooperation with the appropriate authorities
- Ensuring that all user accounts meet Pratt eligibility requirements

## STANDARD PROCEDURES THAT ARE FOLLOWED AT ALL TIMES

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

- Network activity is reported that violates Institute policies, or state or federal laws
- A report is received that materials are posted on Pratt-owned computers, or computers inside the Pratt domain that violate Institute policies, or state or federal laws

- An incident is reported of the commercial use of Pratt-owned computers, or computers inside the Pratt domain, if the commercial activity uses Pratt’s network services

## **POLICY VIOLATIONS**

Violations of the computer usage policy include (but are not limited to) using Institute computers or networks to do the following:

- Harass, threaten, libel, slander, or otherwise cause harm to individuals or groups whether by direct or indirect means
- Destroy or damage hardware, software, or data belonging to the Institute or its members
- Disrupt the activities of others through the unauthorized monitoring of electronic communications
- Copy, download, or transmit across Pratt’s network illegal, proprietary, or unauthorized copyright-protected material
- Use Pratt’s trademarks, logos, or copyrights without prior approval
- Execute software programs that harass other users, infiltrate computers or computing systems, damage or alter software components of a computer or computing system, or introduce computer viruses
- Gain unauthorized access to other systems, facilities, or data either directly or via the network
- Tamper with others’ files, storage media, passwords, and accounts
- In any way misrepresent yourself when sending messages or engaging in conferences
- Conduct any commercial activity over the Pratt network
- Use email to solicit sales or conduct business such as setting up a web page to advertise or sell a service, or posting an advertisement to a news group
- Violate any state or federal law

## **REPORT VIOLATIONS IMMEDIATELY—IT’S FOR YOUR OWN PROTECTION**

All reports of possible violations of this policy will be acted upon quickly and with confidentiality and discretion. Should you believe that a violation of this policy has occurred, immediately report the incident to the Director of Academic Computing.

In addition, contact Pratt Security if you believe that an individual’s health or safety may be in jeopardy.

## **HOW YOUR COMPLAINT WILL BE HANDLED**

Once a complaint is received, the Director of Academic Computing may request authorization to access information contained in the alleged offender’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 notified as soon as possible. If the complaint appears to have merit, the Judicial Affairs Coordinator or Vice President of Student Affairs will meet with the alleged offender and follow the Institute’s judicial procedural guidelines.

## **CONSEQUENCES OF VIOLATIONS**

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

## **ADDITIONAL INFORMATION AVAILABLE FOR STAFF AND FACULTY**

Staff and faculty are referred to the appendix geared to employees that provides additional information on specific policies affecting them. In addition, staff members who oversee server accounts, other than regular accounts, are referred to the appendix on server accounts and Internet accessibility. Both these appendices are available in the offices of Human Resources, the Provost, and the Director of Academic Computing.

## GLOSSARY OF TERMS

**Pratt Institute Computing and Network Resources** (all hardware, software, and data that support the following systems and uses)

- Administrative information systems
- Desktop computers and servers
- Library automation
- Multimedia, data, video, and voice networks
- Electronic mail (email)
- Internet access
- Modems, scanners, telephone systems, voice mail, copy machines, fax machines
- Electronic publications including video

### User

Any person authorized to use the Institute's computing and network resources.

### Authorized Account

An Institute-issued username/password pair or similar codes or code devices such as copy cards that allow a person access to Institute servers and networks.

### CERT (Computer Emergency Response Team)

Initiated to provide 24-hour coverage in the event of a server or network emergency, specifically network intrusions.

## WHERE TO FIND FURTHER INFORMATION

- Pratt Institute Student Handbook
- Pratt Institute Internet User's Guide ([www.pratt.edu/policies](http://www.pratt.edu/policies))
- Appendices (available in the offices of Human Resources, the Provost, and the Director of Academic Computing.)

## WHOM TO CALL WHEN YOU NEED HELP

Call or email these offices if you have questions in the following areas:

### POLICY ISSUES

#### Student Affairs

[stuaff@pratt.edu](mailto:stuaff@pratt.edu)

718.636.3722

### COMPUTERS AND NETWORKS

#### For Technical Support and Computer-Related Questions

[services@pratt.edu](mailto:services@pratt.edu)

718.636.3765

### HEALTH OR SAFETY

#### Pratt Security

[security@pratt.edu](mailto:security@pratt.edu)

718.636.3540

## GENERAL

### Human Resources

[hr@pratt.edu](mailto:hr@pratt.edu)

718.636.3787

## EDUCATION, FREEDOM OF EXPRESSION, RESPONSIBILITY

Pratt Institute's mission is to educate men and women to become creative, responsible professionals who will contribute fully to society. The Institute supports and upholds freedom of speech and other forms of expression because these freedoms are essential to our educational mission. However, we also recognize that the exercise of these rights must not deny the same rights to others.

## COMPUTER SYSTEM IS A RESOURCE FOR ALL

We believe that access to the Institute's computer and network resources is not simply a right but a privilege. We take seriously our obligation to assure the integrity of the systems and the protection of data contained within them. We also take seriously the obligation to protect the Institute, our students, staff, and faculty from legal and other liabilities that might arise from misuse of the computer systems.

#### Vice President for Student Affairs

718.636.3639

#### Director of Human Resources

718.636.3787

#### Director of Academic Computing

718.636.3603

**Pratt**

Pratt Institute  
200 Willoughby Avenue  
Brooklyn, NY 11205

1075\_08\_05