



RUTGERS POLICY

Section: 10.3.11

Section Title: Student Services & Other Student-Related Policies and Programs

Policy Name: Communication to Students

Approval Authority: Executive Vice President for Academic Affairs

Responsible Executive: Executive Vice President for Academic Affairs

Responsible Offices: Office of Student Affairs

Originally Issued: July 29, 2008

Revisions: 4/17/13; 7/1/2013; 7/29/2013

Errors or Changes? Contact: Office of Student Affairs at 848-932-8576

1. **Policy Statement**

Communication to students should be done using email whenever possible. Other forms of conveyance should be used only when necessary.

Communication to students should employ a single means of conveyance unless there is a compelling reason to employ multiple means of conveyance.

It is expected that students will check their email daily.

All university students are required to obtain a Net-ID and official email address.

Students are required to review university communications at least weekly.

2. **Reason for Policy**

The convenience, speed, cost-effectiveness, reliability, ubiquity, and environmental advantages of electronic communications (e.g., email) make it possible to communicate with students more cost effectively than has been possible in the past. Making email the preferred means of conveying information to students enables the University to effectively use its resources to quickly and easily disseminate university-related information and provide students with timely access to that information.

3. **Who Should Read This Policy**

All members of the university community

4. **Related Documents:**

Acceptable Use Policy for Computing and Information Technology Resources, Section 70.1.1 Rutgers Identity Theft Compliance Policy, Section 50.3.9

5. **Contacts:**

For general policy questions contact the Office of Student Affairs 848-932-8576.

For questions relating to Net-ids or obtaining a Rutgers email address contact:

New Brunswick Computing Services New Brunswick Help Desk
848-445-HELP(4357)
helpdesk@nbcs.rutgers.edu <http://www.nbcs.rutgers.edu/helpdesk>

Newark Computing Services Newark Help Desk
973-353-5083
help@newark.rutgers.edu <http://www.ncs.rutgers.edu/helpdesk>

Camden Computing Services Camden Help Desk
856-225-6274
help@camden.rutgers.edu

6. **Policy**

10.3.11 COMMUNICATION TO STUDENTS

Communication to students should be done using email whenever possible. Other forms of conveyance should be used only when necessary.

Communication to students should employ a single means of conveyance unless there is a compelling reason to employ multiple means of conveyance.

This policy provides guidelines for the registration of official addresses and protection of confidential information.

I. Student Registration of Official Addresses:

- A. All students are required to register a Net-ID and password (<https://netid.rutgers.edu>) as well as an official email address (<https://www.acs.rutgers.edu/studentdir/>). A student's email address can be provided by any Independent Service Provider (ISP) and need not be, but can be, a Rutgers email address. Rutgers will make available an email address to any student who requests one. To obtain a Rutgers email address visit <http://oit.rutgers.edu/accounts>.
- B. It is expected that students will check their email daily.

II. Managing Non-public Personal Information

Non-public personal information is any data or information considered to be personal in nature and not subject to public availability. It is the university's policy to protect personal information it receives, handles, and stores, and to comply with the "New Jersey Identity Theft Prevention Act". See Rutgers Identity Theft Compliance Policy, Section 50.3.9.

An individual or unit shall not e-mail data containing non-public personal information to another unit, private entity or public entity over the network unless an encrypted network transmission is used. Non-public personal information includes, but is not limited to:

- a. Social Security numbers
- b. Credit or debit card numbers
- c. State identification card or driver's license numbers
- d. Dates of birth
- e. Health records when the disclosure of the information in question would reasonably be considered to be harmful or an invasion of privacy

Units sending non-public personal information to students are responsible for protecting that information from unauthorized access, modification, or disclosure.

Any messages that contain non-public personal information should be sent using a method that provides the security appropriate for the task. When an electronic message must contain non-public personal information it should only be sent using a secure system that encrypts all transmitted data and requires the user to login with a password to access that data.