RUTGERS ROBERT WOOD JOHNSON MEDICAL SCHOOL
NEW BRUNSWICK, NEW JERSEY

GRADUATE MEDICAL EDUCATION MANUAL

POLICY#: XI.3
SECTION: INSTITUTIONAL POLICIES RELEVANT TO GME
SUBJECT: RIGHTS & RESPONSIBILITIES FOR THE USE OF THE UNIVERSITY ACCESSED ELECTRONIC INFORMATION SYSTEM

I. PURPOSE

To set policy for the use of the University's electronic information systems, broadly defined, including users' rights and responsibilities.

II. APPLICABILITY

A. This policy applies to all individuals accessing and using computing, networking, telephony and information resources through any facility of the University. These individuals include students, faculty, visiting faculty, staff, volunteers, alumni, persons hired or retained to perform University work, external individuals and organizations, and any other person extended access and use privileges by the University under contractual agreements and obligations or otherwise.

B. This policy covers all computing, networking, telephony and information resources owned by, procured through, operated or contracted by the University. Such resources include computing and networking systems (especially those connected to the University's telecommunications infrastructure---the University-wide and campus-wide backbones---as well as local area networks), public-access sites, shared computer systems, personal desktop computers, other computer hardware, software, databases stored on or accessible through the network, IST support personnel and services, physical facilities, and communications systems and services.

III. ACCOUNTABILITY

Under the President, the Senior Vice President for Academic Affairs and the Vice President for Information Services & Technology (IST) shall ensure compliance with this policy. The Deans, Vice Presidents, IST Directors, associate deans for student affairs, and individual managers shall implement the policy.

IV. DEFINITIONS

A. The Internet is a combination of international, national, state and local electronic networks employing a common set of protocols that enables people around the world rapidly and easily to access and exchange information, regardless of origin or location, and provide and receive services.

B. The World Wide Web is a client/server environment on the Internet that provides multimedia information and services with hypertext navigation.

V. REFERENCES - Rutgers Biomedical and Health Sciences Policies:

A.	Information Management	00-01-10-30:00
B.	Patient Confidentiality & Health Information	00-01-40-60:00
C.	Intellectual Property: Copyrights & Royalties	00-01-20-21:00
D.	Sexual Harassment	00-01-35-25:00

VI. EXHIBITS

A. UMDnet Account Holder Use Agreement

B. Academic Computing Services Accounts Policy

C. Academic Computing Services E-mail Policy

VII. POLICY

A. General Principles:

1. The University owns its computing, networking, telephony and other communications systems and its information resources, and has the right to monitor them. The University also has various rights to the software and information residing on, developed on, or licensed for these computers and networks. The University has the responsibility for the security, integrity, maintenance and confidentiality of the electronic systems.

2. Computing, networking, telephony and information resources of the University, including access to local, national and international networks, exist to support students, faculty and staff as they carry out the education, research, health-care and public-service missions of the University, and its administration and management. Toward these ends, the University encourages and promotes the use of these resources by the University community. Access to and use of these resources for purposes or activities which do not support the University's missions are subject to regulation and restriction to ensure that they do not interfere with legitimate work; and any access to or use of these resources and services that interferes with the University's missions and goals is prohibited.

3. When demand for computing, networking, telephony and information resources exceeds available capacity or resources, priorities shall be established for allocating the resources, with a higher priority to activities essential to the missions of the University. The Deans and Vice Presidents, in conjunction with the Vice President for IST, shall set these priorities.

4. Data stewards and system administrators shall develop and publicize specific written procedures to protect the rights of legitimate authorized users, to protect the integrity of the information and systems under their management, and to delineate the responsibilities of users. The University has the authority to control or refuse access to anyone who violates these procedures or threatens the rights of other users or the availability and integrity of the systems and the information. Actions that may be taken under this authority include deactivating accounts, access codes or security clearances; stopping processes; deleting affected files; and disabling access to computing, networking, telephone and information resources.

5. Users' expectation of electronic privacy must be balanced against the University's reasonable need to supervise, control and operate the University's information systems.

6. The University does not archive E-mail that has been sent or received by its systems. The user is responsible for archiving E-mail messages that the user wishes to retain.

B. Rights of Users:

1. Privacy and confidentiality: Because the primary use of the University's communications systems is to further the University's missions, members of the University community should not have the expectation of privacy in their communications, whether work-related or personal. By their nature, electronic communications, especially E-mail connected to the Internet, may not be secure from unauthorized access, viewing or infringement. Although the University employs technologies to secure certain categories of electronic messages, as a rule confidentiality of E-mail and other electronic documents cannot be assumed. The University cannot and does not make any guarantee, explicit or implied, regarding the confidentiality of E-mail and other documents and messages stored in electronic media unless provisions, approved and maintained by the University, are specifically implemented to this purpose. Users should not expect total privacy when using E-mail.

   Although the University will not monitor the content of electronic documents or messages as a routine matter, it reserves the right to examine all computer files in order to protect individuals and the University. In addition, during the course of routine conduct of University business, routine management of the University's computing and networking systems, as well as during emergencies, the University has the right to view or monitor users' files, data, messages or other activity for legitimate business purposes, with or without notice to users. Information seen in such a manner will ordinarily be kept confidential, but may under certain circumstances be used in disciplinary proceedings if appropriate. If an individual is suspected of violations of his/her responsibilities as described in this policy or of other misconduct, the University reserves the right to take any and all actions to abide by the law and maintain network integrity and the rights of access of others

authorized to use the system. The University also reserves the right to access and disclose messages, data, files, and E-mail back-up or archives, if such exist, to law enforcement authorities and others as required by law, to respond to legal processes, and to fulfill its obligations to third parties. E-mail is subject to legal discovery during the course of litigation, even if deleted, by means of message archives, back-up tapes and undeleting the messages.

Therefore, good judgment dictates the creation only of electronic documents that may become public without embarrassment or harm.

2. Safety: Unwanted communications and offensive or objectionable materials are available through the Internet and may be blocked or regulated by the University. The University accepts no responsibility for the content of electronic mail received. However threatening, harassing or offensive communications received by University personnel over the network should be reported to IST, Public Safety and, if appropriate, to the Office of Affirmative Action/Equal Employment Opportunity.

3. Intellectual freedom: The network is a free and open forum for the expression of ideas. The University will not prevent expressions of academic opinions on the network as long as these opinions are not represented as the views of the University and are not in conflict with University policies or state and federal laws. Even with disclaimers about not representing the views of the University, appropriate language, behavior and style should still be used in communications distributed on the University's computing and networking facilities. It should be remembered that certain categories of speech---defamation, obscenity and incitement to lawlessness---are not protected by the Constitution. The University reserves the right, at its sole discretion, to decline to post, to remove posted pages or to restrict University Web sites or computer accounts which contain or are used for personal expressions of a non-academic nature.

C. Responsibilities of Users:

1. Individuals with access to the University's computing, networking, telephony and information resources have the responsibility to use them in a professional, ethical and legal manner. Users are required to take reasonable and necessary measures to safeguard the operating integrity of the systems and their accessibility by others, while acting in a manner to maintain an academic and work environment conducive to carrying out the University's missions efficiently and productively. Specifically, responsibilities of users include:

   a. Respecting the rights of others, including intellectual property, privacy, freedom from harassment, and academic freedom;

   b. Safeguarding the confidentiality of certain information and the privacy of patients;

c. Using systems and resources so as not to interfere with or disrupt their normal operations or their access use and use by others so authorized;

d. Protecting the security of University electronic systems and the integrity of information stored there;

e. knowing and obeying University and unit-specific policies and procedures governing access and use of electronic systems information.

2. Individuals are prohibited from sharing passwords or log-in IDs or otherwise giving others access to any system for which they are not the data stewards or system administrators with appropriate authority. Users are responsible for any activity conducted with their computer accounts and are responsible for the security of their passwords.

3. Individuals may not use another person's network account or try to obtain password or access code to another's network account to send or receive messages.

4. Individuals must identify themselves and their affiliation accurately and appropriately in electronic communications and may not disguise the identity of the network account assigned to them or represent themselves as someone else.

5. The University's communications systems may not be used to harass, intimidate, threaten or insult others; to interfere with another's work or education; to create an intimidating, hostile or offensive working or learning environment; or to conduct illegal or unethical activities.

6. The University's networks may not be used to gain or attempt to gain unauthorized access to remote networks or computer systems.

7. Individuals are prohibited from deliberately disrupting the normal operations of the University's computers, workstations, terminals, peripherals or networks.

8. Individuals may not run or install on any University computer system a program that may result in intentional damage to a file, or that may intentionally compromise the integrity of the University's systems or the integrity of other computing environments via the University's network (e.g., computer viruses, Trojan horses, worms or other rogue programs).

9. Individuals are prohibited from circumventing access and use Authentication systems, data-protection mechanisms, or other security safeguards.

10. Individuals must abide by all applicable copyright laws and licenses, and respect other intellectual-property rights. Information and software accessible on the Internet is subject to copyright or other intellectual-

property-right protection. University policy and the law forbid the unauthorized copying of software that has not been placed in the public domain and distributed as "freeware." Therefore nothing should be downloaded or copied from the Internet for use within the University unless express permission to do so is stated by or received from the owner of the material, and the owner's requirements or limitations on use of the material are observed. The use of software on more than the licensed number of computers, unauthorized installation of unlicensed software on University computers, plagiarism and invasion of privacy are also prohibited. "Shareware" users must abide by the requirements of the shareware agreement.

11. Activities that waste or unfairly monopolize computing resources (such as unauthorized mass mailings; electronic chain letters, junk mail and other types of broadcast messages; unnecessary multiple processes, output or traffic; exceeding network directory space limitations; excessive game-playing or other trivia applications; and excessive printing) are prohibited.

12. Reading, copying, changing or deleting programs or files that belong to another person or to the University without permission is prohibited.

13. The University's computing resources may not be used for commercial purposes or personal financial gain.

14. All network communications exiting the University are subject to the acceptable-use policies of the network through which they flow.

15. Use of the University's systems that violates local, state or national laws or regulations or University policies, standards of conduct, or guidelines is prohibited.

16. Confidential information should be encrypted before transmission over open public networks such as the Internet, or such transmission should only be over secure dedicated lines. Including confidential University information in unencrypted E-mail is forbidden.

D. E-mail and other electronic communications (Internet services, voice mail, audio- and video-conferencing, and facsimile messages):

1. The use of University resources for electronic communications must be related to University business, including academic pursuits, and not for personal or commercial purposes, except for incidental and occasional personal non-commercial use when such use is clearly insignificant, does not generate a direct cost for the University, and does not interfere with or compete with legitimate University business.

2. Only authorized persons may use the University's electronic communications systems.

3. Electronic communications whose meaning, transmission or distribution is illegal, unethical, fraudulent, defamatory, harassing or irresponsible are

prohibited. Electronic communications should not contain anything that could not be posted on a bulletin board, seen by unintended viewers, or appear in a University publication. Material that may be considered inappropriate, offensive or disrespectful to others should not be sent or received as electronic communications using University facilities.

4. Appropriate standards of civility and decency should be observed in electronic (as well as all other forms of) communication.

E. World Wide Web:

1. "Official" University Web pages are those that provide information about established, University-recognized entities, such as its Schools; patient-care units; administrative offices; research institutes, centers and programs; educational programs; clinical centers, institutes and programs. Information on official University Web pages represents the institution and therefore must be accurate, timely and useful and must conform to this and all other University policies, standards and requirements. Official Web pages shall be held to the same standards as any University, school or unit printed publication.

    a. The pertinent Dean, Vice President or Department Chair has the ultimate responsibility for official Web pages. These individuals or their designees must authorize the establishment of any official Web page under their purview.

    b. The University logo must appear on all official Web pages, or their equivalent.

    c. Official RUTGERS Robert Wood Johnson Medical School Web pages shall be reviewed by the responsible party every six to twelve months and these reviews documented by changing the revision date at the bottom of the page.

    d. Official RUTGERS Robert Wood Johnson Medical School pages may be copyrighted. Official RUTGERS Robert Wood Johnson Medical School Web pages should not contain copyrighted materials without appropriate copyright permission.

2. Faculty professional Web pages and personal Web pages of a faculty member, student or staff member may not: promote illegal activities; harass anyone inside or outside the University; include offensive or objectionable material or language or link to other sites that do; distribute copyrighted materials; be used for commercial purposes or personal gain unrelated to the University's missions; contain the University logo; represent the contents as being the official policy or positions of the University. Personal pages from individuals or groups must include the identity of the author, and should contain the following statement: "The views and opinions expressed in this page are strictly those of the author. The contents have not been reviewed or approved by the RUTGERS

Robert Wood Johnson Medical School." The University reserves the right to not post or remove posted pages for any reason.

F. Non-compliance and Sanctions:

Non-compliance with this policy may result in denial or removal of access privileges to the University's electronic systems; disciplinary action under applicable University policies and procedures; civil litigation; and/or criminal prosecution under applicable state and federal statutes.

By Direction of the President:

_____

Vice President for Information Services and Technology

EXHIBIT A

UMDnet Account Holder Use Agreement
http://www.RUTGERS Robert Wood Johnson Medical School.edu/istweb/prodserv/acs_use.htm
August, 1999

As a UMDnet account holder of the RUTGERS Robert Wood Johnson Medical School, ("University"), and as a user of the computing and communications facilities of the University, I agree to observe the University Policy on Rights & Responsibilities for the Use of University-accessed Electronic Information Systems, the Academic Computing Services Email Policy and the following rules and regulations governing the use of same:

1. Only I will use the computer User Account(s) provided to me and I will take the responsibility to protect my account(s) from unauthorized access. I will not allow anyone else to use my User Account. I understand that I will be requested to change my password at thirteen week intervals, although I may elect to do so at more frequent intervals if I believe that the privacy of my password has been compromised. This rule is primarily intended for the protection of my User Account(s) and its data.

2. If I have information regarding attempts to breach the security of the University's computer facilities, I agree to promptly report such information to the Department of Information Services and Technology.

3. I shall respect the privacy of information on the University's computing facilities. I shall not attempt to access any data or programs that I do not own unless they have been made publicly available or I have the express permission of their owner. I shall make no attempt to modify data or program material available for general (public) use without the permission of the owner.

4. I agree to abide by any patent or copyright restrictions which may relate to the use of computing facilities, products, programs or documentation. I agree not to copy, disclose, modify or transfer any such materials that I did not create, without the expressed consent of the original owner or copyright holder. I agree not to use the University's computing facilities in any way which violates the terms of any software license agreement; applicable local, state or federal laws or University policy.

5. Facilities are available for the conduct of University business, i.e., research, instruction, health care and administration. No other uses are permitted.

6. I shall not use the University's computing facilities for any form of private financial gain. Business pursuits other than those outlined in 5. above will require special approval from IST along with approval of the requester's department. A separate, billable account may be established depending on the nature of the proposed use.

7. I understand that access to the University's computing facilities by unauthorized persons or for unauthorized purposes is forbidden. I shall not use University computing facilities in any way that intentionally compromises their availability or effectiveness to other individuals. Some examples are presented for clarification:

Attempts to access restricted portions of an operating system, accounting software or the private file space of other users;

Use of information systems in such a way as to disrupt the operation of computer or communication systems within or outside of the University;

Attempts to breach security mechanisms or exploit or publicize problems that might exist in them;

Failure to abide by policy posted at public computer centers.

8. I shall not use my computer account privileges to attempt access to computing facilities within or external to the University to which I have not received prior authorization.

9. I agree to abide by any and all other rules and regulations of the University regarding the use of its computer facilities, now in effect or hereinafter enacted by the University.

10. I understand that non-compliance with this Agreement may result in denial or removal of access privileges to the University's electronic systems; disciplinary action as set forth by other University policies and guidelines, civil litigation; and/or criminal prosecution under applicable state and federal statutes. I agree to be personally liable for all claims, lawsuits and damages to the University which result from my breach of this Agreement. The terms of this section 10 will survive the termination of this Agreement.

11. I agree to immediately notify the RUTGERS Robert Wood Johnson Medical School Information Services & Technology Department to terminate my account in the event that I am no longer employed by, a student at or affiliated with the University.

This agreement will remain in force as long as I have a UMDnet Account.

Print Name	Signature	Today's Date

Employee: Unit/School and Department	Student: School and Graduation Year

EXHIBIT B

Academic Computing Services Accounts Policy

http://www.RUTGERS Robert Wood Johnson Medical School/edu/istweb/prodserv/acs_acpl.htm
August, 1999

Eligibility

1. All salaried RUTGERS Robert Wood Johnson Medical School full-time faculty or staff.

2. All students enrolled or matriculated in a RUTGERS Robert Wood Johnson Medical School or program.

3. Other students enrolled in a single RUTGERS Robert Wood Johnson Medical School course - eligible for temporary accounts.

4. RUTGERS Robert Wood Johnson Medical School part-time or voluntary faculty or other volunteers who have a demonstrated need for computer resources available from ACS (other than general Internet access) in connection with their work at the University - eligible for temporary accounts.

5. Employees or students of affiliated hospitals or educational institutions that have relationships with RUTGERS Robert Wood Johnson Medical School departments and have a demonstrated need for computer resources available from ACS (other than general Internet access) in connection with their responsibility at the University - eligible for temporary accounts.

6. Affiliated organizations with an academic or health care mission whose activities in connection with the University require computing resources the affiliate cannot reasonably supply on its own - eligible for temporary accounts.

Applying for an ACS Computer Account on a RUTGERS Robert Wood Johnson Medical School Campus Host

1. In person at one of the following campus Academic Computing Labs:

   a) Newark: MSB Room C632
   b) Piscataway: RWJMS Room N217
   c) New Brunswick: MEB RWJ Library of the Health Sciences
   d) Camden: E&R Bldg Room 140A in the RUTGERS Robert Wood Johnson Medical School and Coriell Research Library
   e) Stratford: Academic Center Room 247
   f) Scotch Plains: Room 319

2. By phone, call your campus Academic Computing Lab Support Desk:
   a) Newark: 2-6789 (973-972-6789)
   b) Piscataway: 5-4436 (732-235-4436)
   c) New Brunswick: 5-7773 (732-235-7773)
   d) Camden: 7-7875 (856-757-7875)
   e) Stratford: 6-3200 (856-566-6437)
   f) Scotch Plains: (908-889-2447)

Obtaining Account Name and Password

1. In person at one of the following campus Academic Computing Labs:
   a) Newark: MSB Room C632
   b) Piscataway: RWJMS Room N217
   c) New Brunswick: MEB RWJ Library of the Health Sciences
   d) Camden: E&R Bldg Room 140A in the RUTGERS Robert Wood Johnson Medical School and Coriell Research Library
   e) Stratford: Academic Center Room 247
   f) Scotch Plains: Room 319

2. Present one of the following:

   a) RUTGERS Robert Wood Johnson Medical School ID - for individuals satisfying items 1 or 2 of the eligibility requirements.

   b) For individuals satisfying items 3, 4, or 5 of the eligibility requirements, a letter signed by your RUTGERS Robert Wood Johnson Medical School department chair, faculty sponsor, or course director stating:

      1) You are working for/affiliated with a RUTGERS Robert Wood Johnson Medical School department or enrolled in a RUTGERS Robert Wood Johnson Medical School course.
      2) The intended uses for the account and the IST/ACS resources required for your work/class.
      3) The period for which the account will be necessary (cannot exceed one year).

   c) For individuals satisfying item 6 of the eligibility requirements, a letter signed by a senior official of the affiliated organization stating the resources needed not available through the affiliated organization.

3. Read and sign the UMDnet Account Holder Use Agreement form (http://www.RUTGERS Robert Wood Johnson Medical School.edu/istweb/prodserv/acs_use.htm). This details the acceptable uses of the IST/ACS' computational and information services and must be strictly adhered to.

Temporary Accounts

Temporary accounts are given to individuals satisfying items 3, 4, 5, or 6 of the eligibility requirements. The account will be opened for the specified time period determined by the individual's needs and will not exceed one year. Temporary accounts will expire automatically. In order to renew the account the individual must re-apply in person.

Alumni Accounts

Alumni accounts are given to all RUTGERS Robert Wood Johnson Medical School graduates. These are non-interactive email accounts with Internet access and only are accessible through a SLIP/PPP connection using client software (ex. web browsers, email clients). You cannot connect to these accounts by telnet or other "terminal" protocols. If the account shows no activity for twelve months it will be deleted permanently. If you forget your password the account

will eventually age out after twelve months. Passwords cannot be reset for these alumni accounts.

Deactivating and Removing Accounts

1. An account will remain active providing that the account holder continues to meet the eligibility requirements, the account is accessed directly through a campus host login (ex. telnet) at least once in a 6 month period and the account is renewed prior to its expiration (temporary accounts). To reactivate the account, you must go in person with your RUTGE Robert Wood Johnson Medical School ID to your campus Academic Computing Lab.

2. An account will become non-interactive if, within a 6 month period, the only method of access is through client software (ex. web browser, email client). Once an account becomes non-interactive, you cannot run terminal sessions; however, you can continue to use your client software. To reinstate direct access to your account, you must go in person with your RUTGERS Robert Wood Johnson Medical School ID to your campus Academic Computing Lab.

3. An account will be deactivated if it is not accessed at least once in a 6 month period through a resource that requires authentication (ex. telnet, remote access via SLIP/PPP). Note: LAN logins in an Academic Computing Center do not prevent the account from being deactivated. To reactivate an account, you must go in person with your RUTGERS Robert Wood Johnson Medical School ID to your campus Academic Computing Lab.

4. An account will be removed for any of the following reasons:

   a) The account holder no longer meets the eligibility requirements.
   b) The account is established as temporary and the expiration date has been reached without renewal.
   c) The account has not been accessed in 13 consecutive months.
   d) The account holder is in violation of the UMDnet Account Holder Use Agreement (http://www.RUTGERS Robert Wood Johnson Medical School.edu/istweb/prodserv/acs_use.htm), the Academic Computing Services Email Policy (http://www.rutgers.rwjms.edu/istweb/prodserv/acs_empl.htm) and/or the University Policy on Rights & Responsibilities for the Use of University-accessed Electronic Information Systems.

Passwords

1. Accounts will be opened with a pre-assigned password that must be changed upon logging in for the first time.

2. Passwords must conform to the following rules:

   a) Passwords must be 6, 7 or 8 characters in length and contain at least one non-alphabetic character. It is suggested that passwords be a combination of lowercase alpha characters and numbers.

b) Avoid the use of names such as hostname, account name, real name or any other information associated with your account. Avoid words that can be found in a dictionary.

c) Passwords with an embedded word of a length greater than 3 or with 3 or more repeated characters will be rejected.

d) A new password must differ from the old password by at least three characters.

e) Passwords must be changed every 13 weeks. To make a password eligible for re-use, the password must have been followed by a succession of at least 3 password changes and at least 1 year must have elapsed since it was last used.

3. Passwords cannot be retrieved from the system. If a password is forgotten the account holder must visit in person one of the listed Academic Computing Labs where a valid RUTGERS Robert Wood Johnson Medical School ID or proper identification must be presented. A new password will be issued. Call your campus Academic Computing Lab for the appropriate procedure on your campus.

4. Passwords automatically expire every 13 weeks. You will be prompted to change your password after logging in. You may elect to change your password at more frequent intervals and should do so if you believe that the privacy of your password has been compromised.

5. It is strictly forbidden to share or divulge passwords.

EXHIBIT C

Academic Computing Services Email Policy
http://www.rutgers.rwjms.edu/istweb/prodserv/acs_empl.htm
August, 1999

In accordance with the University Policy on Rights & Responsibilities for the Use of University-accessed Electronic Information Systems:

"Individuals with access to the University's computing, networking, telephony information resources have the responsibility to use them in a professional, ethical and legal manner. Users are required to take reasonable and necessary measures to safeguard the operating integrity of the systems and their accessibility by others, while acting in a manner to maintain an academic and work environment conducive to carrying out the University's missions efficiently and productively."

"Electronic communications whose meaning, transmission or distribution is illegal, unethical, fraudulent, defamatory, harassing or irresponsible are prohibited. Electronic communications should not contain anything that could not be posted on a bulletin board, seen by unintended viewers or appear in a University publication. Material that may be considered inappropriate, offensive or disrespectful to others should not be sent or received as electronic communications using University facilities."

I. Actions Considered Violations of the UMDnet Account Holder Use Agreement (http://www.rutgers.rwjms.edu/istweb/prodserv/acs_empl.htm):

Sending unsolicited bulk email messages ("junk mail" or "spam") which is disruptive or generates a significant number of user complaints.

Sending email to any person whom does not wish to receive it.

Harassment, whether through language, frequency, content or size of messages.

Forwarding or otherwise propagating chain letters and pyramid schemes, whether or not the recipient wishes to receive such mailings.

Malicious email, such as "mailbombing" or flooding a user site with very large or numerous pieces of email.

Forging of sender information other than accountname@rutgers.rwjms.edu or other pre-approved header address.

Sending email for commercial gain.

IST has the right to remove access to accounts found in violation of this policy.

II. Email Rules & Controls:

A size limitation of 4MB for ALL email messages addressed to accountname@RUTGERS Robert Wood Johnson Medical School.edu whether they originate from within or outside of the University.

Email messages through the ACS campus hosts will be blocked where neither the sender nor the recipient's address belongs to RUTGERS Robert Wood Johnson Medical School

The inclusion of patient-identifiable information in unencrypted email is forbidden.

The University does not archive email.

For ACS campus host accounts only:

A size limitation of 4MB for outgoing (sent) messages.

Received messages may not exceed 4 MB.

Messages will be removed from INBOX when they are older than 45 days.

When an account becomes deactivated all incoming mail will be returned to sender as "undeliverable".

User accounts have a quota of 4MB of space and 200 files. Users are requested to clean up the folders where they store copies of outgoing and incoming email periodically.

Note: Junk mail sent directly to a RUTGERS Robert Wood Johnson Medical School.edu address from the outside is not preventable. It should be treated like junk US postal mail. Filters are available and may be used on an individual basis with the understanding that side effects such as filtering out "good" mail might occur. ACS provides boilerplate filters and instructions in the use of filtering programs. Some mail programs that run on your own computers also offer filtering capabilities.

Rutgers Biomedical and Health Sciences Policy Code: 00-01-10-40:00

Adopted: 8/31/99

Amended: 2/08/00

Approved by GMEC on 1/11/00