PURPOSE

To ensure appropriate use of all RML Specialty Hospital (RML) computing resources.

PROCEDURE

The framework of responsible, considerate, and ethical behavior expected by RML extends to cover use of all RML computers and workstations, programs, use of RML network resources, and use of any future computing resources provided by RML. The following list does not cover every situation that pertains to proper, or improper, use of the resources, but it does suggest some of the responsibilities which you accept if you choose to use an RML computing resource.

1. RML makes available computing and network resources which may be used by RML employees and individuals (users) authorized by the Information Services (IS) department only. The resources available are intended to be used to carry out the legitimate business of RML.

2. Those who avail themselves of the system and network computing resources are required to behave in a manner consistent with this policy. All information entered into the computer system must be true and accurate.

3. The computing and network resources of RML may not be used by employees for commercial purposes or for financial gain. Unless approved by Administration, any activity outside the scope of your employment is not allowed.

4. Messages, sentiments, and declarations sent as electronic mail or sent as electronic postings must meet the same standards for distribution or display as if they were tangible documents or instruments. If you would hesitate to put the material on the cafeteria wall and attach your name to it, it is inappropriate. Administration has final authority on what is suitable. You may not alter the “From” line or other attribution of origin in electronic mail.

5. Unauthorized or fraudulent use of the RML computing resources is a serious violation of RML regulations. Duplicating software which is protected by copyright or trade secret law is a violation of the law. You must abide by the terms of all software licensing agreements and copyright laws. In particular, you must not make copies of copyrighted software, unless RML has a site license specifically allowing the copying of that software. Furthermore, you must not copy site-licensed software for distribution to persons or staff, nor may you copy site-licensed software for use at locations not covered under the terms of the license agreement.
6. RML presents for your use many programs and data which have been obtained under contracts or licenses saying they may be used, but not copied, cross-assembled, or reverse-compiled. You are responsible for determining that programs or data are not restricted in this manner before copying them in any form, or before reverse-assembling, or reverse-compiling them in whole or in any part. If it is unclear whether you have permission to copy such software, assume that you may not do so.

7. Because electronic information is volatile and easily reproduced, respect for intellectual labor and creativity is vital. This principle applies to work of all authors and publishers in all media.

8. All programs and data created or entered by IS staff or other RML employees should be considered confidential. The use of such programs and data is limited to the activities necessary to support RML activities only. Users may not sell, transfer, publish, disclose, display or otherwise make available any RML computer programs, copies of programs, or output of programs in any form whatsoever to any person or entity without prior written approval of RML.

9. You must not attempt to decrypt or translate encrypted material, or obtain system privileges to which you are not entitled.

10. You must not attempt to modify in any way a program which RML supplies for any type of use.

11. You must refrain from any action which interferes with the supervisory or accounting functions of the systems or that is likely to have such effects.

12. Attempts to read another person’s electronic e-mail files or other computer files will be treated with the utmost seriousness. The system administrators will not read mail or non-world-readable files unless necessary in the course of their duties. Bounced mail is directed to the system administrators for the purposes of assuring reliable e-mail service.

13. You must not intentionally seek information about, browse, obtain copies of, or modify files, passwords, or tapes belonging to other people, unless specifically authorized to do so by those individuals. (Note: if an individual has explicitly and intentionally established a public server, or clearly designated a set of files as being for shared public use, others may assume authorization.)
14. If you discover that someone has made unauthorized use of your computer, you should change the password and report the intrusion to IS. You should change your password on a regular basis, to assure continued security of your computer. The system will automatically prompt you every 90 days to change your network password. Passwords in application systems should be changed by the user at least as often.

15. Users are responsible for all use of their accounts, including choosing safe passwords (8 characters or more are recommended). Using birth dates or names of significant others, children, and pets is discouraged. Passwords should be kept confidential. Users should not leave their computers logged in and unattended if the possibility exists for someone with no or lower security rights to access the computer.

16. If you encounter or observe a gap in system or network security, you must report the gap to the IS Department. You must refrain from exploiting any such gaps in security.

17. Refrain from sending frivolous or excessive e-mail and from printing excessive copies of documents, files, images or data. You must refrain from using unwarranted or excessive amounts of storage and from printing documents or files numerous times because you have not checked thoroughly for all errors and corrections. You must be sensitive to the special need for software and services available in only one location, and relinquish the place to those whose work requires the special items.

18. You must not prevent others from using shared resources by running unattended processes. Your absence from a public computer or workstation should be no longer than warranted by a visit to the nearest restroom. A device unattended for more than ten minutes may be assumed to be available for use, and any process running on that device terminated. You must not password lock a public workstation or computer.

19. Unclassified data and information may be encrypted only with prior authorization of your supervisor. Whenever encryption is used, your supervisor or IS must be provided the decryption key to ensure that encrypted information on RML systems will be available in the event the user is no longer available to decrypt the information.

20. No data should be stored on local drives of desktop computers located at RML. All data should be saved to appropriate network drives only.

21. If you create or maintain electronically stored information, whether at home or at an RML site, which is important to your work or to RML, you are responsible for making frequent backups of the information. If the information is stored on the network, it will be backed up nightly by IS. The data in the backups must be in a secure environment and not be accessible by non-RML employees/contractors.

22. Upon termination of employment from RML for any reason, you shall immediately surrender to RML all RML property including, without limitation, computer hardware, computer
programs, copies of computer programs, output of computer programs and RML data stored in computer programs.

23. The following type of information or software cannot be placed on any RML computing resource:
   - electronic chain letters
   - that which infringes upon the rights of another person
   - that which is abusive, profane, religiously or sexually offensive
   - that which consists of information which may injure someone else and/or lead to a lawsuit or criminal charges. Examples of these are: pirated software, destructive software, pornographic materials, or libelous statements.

24. You must not run or install on any RML computer system, or give to another, a program that could result in the eventual damage to a file or computer system and/or the reproduction of itself. This is directed towards, but not limited to, the classes of programs known as computer viruses, Trojan horses, and worms.

25. You may not install any commercial, freeware, or shareware software on any RML computer without permission from the IS department. This includes, but is not limited to, screen savers and games.

26. You should not use media used outside of RML. If this is necessary, you must have the media scanned prior to each use. If you are authorized by IS to access external data sources such as the Internet or bulletin boards via modem, all downloaded information must be scanned immediately upon terminating the external connection. You should not turn off the automatic scanning feature of the virus software installed on RML computers.

27. You must be sensitive to the public nature of shared facilities and not display on such screens images, sounds or messages which would create an atmosphere of discomfort or harassment for others (i.e., abusive, profane, or sexually offensive). You must also refrain from transmitting to others in any location inappropriate images, sounds, or messages which might reasonably be considered harassing.

28. You must not make use of any RML system for illegal or criminal purposes.

29. You should be aware that there are Federal, State, and, sometimes, local laws which govern certain aspects of computer and telecommunications use. RML employees are expected to respect these laws, as well as to observe and respect RML rules and regulations.

30. Because these computational resources are RML property, their use may be subject to monitoring, recording, and audits to ensure the systems and networks are functioning properly, to protect against unauthorized access or use, and to ensure the confidentiality and integrity of data and information resident on the systems and networks. In addition, RML’s IS staff may access any user’s computer system or data communications and disclose information obtained through such auditing to appropriate third parties, including law
enforcement authorities. Users have no expectation of privacy when using RML computing resources. Use of an RML computing resource and network connection constitutes express consent by the user to monitoring, recording, and auditing for purposes identified above. Please note: e-mail and electronically stored documents (even those deleted) may be used as evidence in lawsuits.

Responsibilities

A. Employee

1. Adheres to Computer Use Policy.
2. Returns a signed copy of the Computer Use and Security Agreement to his/her Department Manager.

B. Department Manager

1. Signs and forwards all Computer Use and Security Agreements to Information Services.

C. Human Resources

1. Provides new employees with a copy of the Computer Use Policy and the Computer Use and Security Agreement.
2. Notifies Information Services immediately upon a user’s termination with RML.
3. Forwards the signed Computer Use and Security Agreement to IS.

D. Information Services

1. Authorizes computer access only to users with a signed Computer Use and Security Agreement on file.
2. Monitors compliance with Computer Use Policy.

Developed by: Julie Ames, Chief Information Officer

Approval: I/S Steering Committee