LUTHER RICE COLLEGE & SEMINARY

Computer and Technology Use Policies and Procedures
2014-2015

Updated December 2013
(Approved by the President's Council on December 4, 2013)

Contents

Introduction:

Luther Rice University (LRU) is committed to providing a secure computing environment. To ensure that the full potential of the computing environment is realized, it is important that users understand their responsibilities in relation to the use of assets of the Office of Information Technology.

The purpose of this document is to offer guidance to users of computing facilities at LRU and to illustrate some of the issues addressed in the University's Security Policies. These notes are not a complete statement of the law or the University's policies and should be read in conjunction with the text of the University security policies.

The Office of Information Technology facilities at LRU are essential for the University's primary functions of teaching, research, and administration. Their use is governed by these policies and procedures, as well as by related policies detailed below. These policies complement and supplement rather than replace other policies concerning appropriate conduct of students, visitors, and staff.

All users must comply with these policies and procedures. In the event of misuse of the University's information technology systems you may be subject to various actions, which may include, but are not limited to:

- Suspension from use of the system
- Disciplinary action including termination of employment, study, or computer access, depending upon the severity of the infraction
- Personal liability punishable under civil or criminal law

The sections below cover policy and guidelines relating to the following areas of Computer Use:

1. General: policies and guidelines for all users that access the University network.
2. Record retention: obligations with regard to saving and appropriate retention of important electronic information.
3. Email: policy and guidelines relating specifically to the use of email.
4. University-owned technology assets and facilities: policy relating to using such resources as workrooms/labs for students and desktop/laptop computers for staff.
5. Connection of equipment to the University network: policy relating to connection of equipment, including, but not limited to: laptop computers, modems, and routers, to the University network.
6. General Computer Use
7. Email guidelines
8. Guidelines for the connection of equipment to the University network.

Continued on Next Page

Definitions:

IT is an abbreviation for Information Technology and is used as a collective term to describe all systems, services, hardware, and software associated with computers, digital networks, and telecommunications.

OIT is an abbreviation for Office of Information Technology and is used as a collective term to describe functions and or services that originate in the Office of Information Technology.

Network Device includes, but is not limited to: routers, switches, analogue modems, DSL modems, wireless access devices, computers acting as DHCP servers, DNS servers, File Servers, Mail Servers. The term does **not** include general purpose computers, laptops, tablets, PDAs, and similar personal devices.

System and **Computer System** include any University computer system, local area, and telecommunications networks controlled, operated, or authorized by any College, Faculty, School, Department member of the University, or by the University administration. These terms include any part of the foregoing items and all related input, output, processing, storage, software, communications facilities, and stored data.

Network Administrator, System Administrator, and **System Manager,** in relation to any system, means the person or persons authorized to maintain and control the system.

User is any authorized person accessing or using LRU Information Technology assets or facilities.

Username and **IT Account** are synonyms that refer to the personal computer identity that is given to you when you join the University. It has an associated password that is private. The username and password are used to authenticate a user on particular systems and services and also for IT resource charging purposes. Username also refers to any username allocated separately by a College, School, or Department.

Policy Statement:

COMPUTER USE

Note: References after particular policy statements refer to the main guidelines relevant to that part of the policy.

1. General

1.1 You must authenticate using a valid username. [6.1]

1.2 You must not disclose to others any password or other IT account information that could be used to gain access to your own or any other account and you should not use another person's username and password. [6.1]

1.3 You are responsible and financially liable for all computer activity related to your IT account – this includes both incoming and outgoing Internet traffic. [6.2]

1.4 No person shall without authority of the Chief Information Officer:

- access or attempt to gain access to any computer system, asset, or facility;
- in any way obtain, copy, modify, interfere with, attempt to erase, or in any way remove any information from a system;
- use any computer system, technology asset, or facility in such a way as to contravene any requirements for its use as determined by a System Administrator;
- remove, disconnect, tamper, or otherwise interfere with any physical component or components of a computer system or technology asset;
- subvert, or attempt to subvert, any user identification and/or authentication scheme on any system;
- cause or attempt to cause any computer system to fail or deny service to any authorized user;
- assist any person to do any of the above [6.3]

1.5 No person shall use or attempt to use any computer system so as to create costs, expense, or loss, financial or otherwise, to be incurred by:

- the University or any section of the University without the consent of the head of the section concerned;
- any person or organization whether or not a part of, or connected in any way with, the University without the consent of that person or organization [6.3]

1.6 The use of technology assets or facilities to send or disseminate offensive, abusive, threatening, or unnecessarily repetitive messages or material may be considered harassment and fall subject to the University's Harassment Procedures and/or Discipline Regulations. [6.3,6.4]

1.7 You must not use the technology resources for nefarious (wicked or criminal) activities. [6.3,6.5,8.10]

1.8 Log files of all network activities are kept and these log files provide information as to the use of IT components. Such information may be used as evidence of breaches of policy of the Office of Information Technology (OIT). [6.3]

1.9 The contents of computer files and email messages in your allocated disk space will be treated as private. However, you should be aware that this treatment does not necessarily imply legal ownership of the content. For example, the ownership of intellectual property in the content may rest with the University or other parties, and may depend on contracts, statutes, and policy outside this document. Note that System Administrators are authorized to carry out routine system operations on these files and messages, which can involve the examination of their content, at any time. Backup is one such routine operation, therefore privacy is not guaranteed. [6.3]

1.10 System Administrators are authorized to examine, move, copy, or delete any files and email messages when such action is authorized and deemed appropriate — as defined in [6.3, 6.4].

1.11 Any person who, in the opinion of the Chief Information Officer, is engaged in a breach of this policy may be immediately excluded from that system and all associated computer activities suspended. Failure by that person to comply with instructions necessary for exclusion shall in itself constitute a breach of this policy. The exclusion of a student from any system for a cumulative total of more than twenty-four hours when the student is using the system for course work shall be reported to the President of the Institution as soon as is

practicable. The exclusion for a cumulative total of more than one hundred and sixty eight hours of any person from a system shall be reported to the President of the Institution as soon as is practicable. Any person aggrieved by exclusion may appeal within fourteen days of being notified of the exclusion: if a student- to the Vice President of Student Services, and if a staff member- to the President of Luther Rice University. [6.3,6.4,6.5]

1.12 You must conform to the rules and codes of conduct for all IT networks, assets, and systems to which you obtain user account access through the University.

1.13 You may not use your network connection or computing privileges for unauthorized personal use.

2. *Record Retention*

2.1 All electronic records that would normally be saved if they were paper documents should be retained on the same basis.

3. *Email*

3.1 All University staff and students have an official University email address associated with their computer account. You should make sure that email to this address is checked on a daily basis. [7.1,7.2, 7.3]

3.2 You must not use the University's email systems to:

- create or distribute chain letters, "junk" or "spam" (mass, unsolicited) mail;
- send anonymous email;
- disrupt another person's activities;
- harass another person or send unwanted offensive material;
- forge email messages to make them appear to come from another person;
- read, delete, copy, or modify email under the control of other users without authorization;
- pursue commercial activities, including sending "for-profit" messages or advertisements, unless on behalf of the University or its associated organizations;
- introduce viruses or other malware;
- download unauthorized software without approval;
- intentionally engage in illegal activities [6.3,6.4,6.5,7.3]

3.3 You are responsible for all email originating from your account. [7.4,7.5,7.6,7.7,7.8]

3.4 You may not send an email that purports to represent the University or its views, without proper authority. If there is any risk of misunderstanding, a disclaimer must be inserted in your email, especially when the recipients are unknown, such as in discussion lists. [7.5,7.6,7.7]

3.5 All emails sent from the University must go through the LRU email gateway.

4. *Use of University-owned Technology Assets and Facilities*

4.1 University owned computer facilities are provided to support the primary functions of the University and its administration. Personal use is allowed on most University systems but only when the system is not required for its primary functions and, for staff members, only when it does not impede the work for which they are employed.

4.2 The use of computing equipment is integral to many aspects of University study. The equipment should not be interfered with or left in a state that denies others reasonable access.

5. *Connection of equipment to the University network*

5.1 A System Administrator may authorize disconnection of equipment from the network if it is a threat to the integrity of the network either as a result of not adhering to this policy, or because of its behavior. [8.1,8.2,8.6,8.7,8.9,8.10]

5.2 Computers connected to the campus local area network (including by direct Ethernet, wireless, broadband, VPN, or other means) must have up-to-date (within 30 days) virus protection software installed and active at all times; and should have all relevant system security patches installed. The following is a list of supported anti-virus products, and are strongly recommended: Webroot, AVG, Kaspersky, and Microsoft Security Essentials. [8.3]

5.3 You must not remove access, or in any other way block access, of the Domain Administrators to any Windows computer in the "LRU" domain.

5.4 You are responsible, and financially liable, for all traffic originating from a computer connected to the University network and owned by you. [8.4,8.9]

5.5 Computer Names - See the Computer Administration Policy for naming standards for University-owned equipment.

For computers not owned by the University, such as staff-owned and visitors' laptops, you are allowed to choose a name for your computer. This name should not be offensive. The Institution reserves the right to enforce a name change. Non-standard names should be notified to the IT Helpdesk (once only) if they are to be connected to the network for more than one day. [8.5]

5.6 Network Numbers - Unless instructed otherwise by the Network administrators, machines must be dynamically assigned their IP numbers via the Information Technology Services DHCP server(s); you MUST NOT assign IP numbers manually. Additionally, you must not mask or otherwise change your machine's hardware (MAC) address.

5.7 Security and Privacy - Network traffic is private. "Packet sniffing", or other unauthorized and deliberate attempts to read network information, is not permitted. You are responsible for the security and integrity of your computer. [8.7]

5.8 Personal computers may not act as servers to other machines on the Internet. Student machines are not allowed to run Internet servers of any kind. [8.8]

5.9 No Network Devices (including modems) are to be connected to any portion of the network without the express permission of a Network Administrator. [8.11,8.12]

5.10 Routers, Switches and Hubs on Campus. The use of popular small home routers (wireless, cable or DSL) on campus is not necessary and is absolutely prohibited. Any computer misconfigured as a router or set up for home networking that assigns IP addresses will cause problems on the network and will be immediately disconnected. Equipment that acts as an unauthorized DHCP server is strictly forbidden. The use of hubs to allow multiple computers to use the same wall socket is strictly forbidden, without the permission of the Chief Information Officer. [8.11]

5.11 Broadband. No routing software is allowed on any computer that connects the University broadband or dial-in port to any other network communication port. Only one network connection port may be active at any given time.

Procedures and Guidelines:

COMPUTER USE

6. General Computer Use

6.1 A Username is assigned to all LRU employees.

6.2 The use of a Username is for staff only.

6.3 System Administrators may need to examine, move, copy or delete files when there are reasonable grounds to believe, for example:

- that the integrity of the system or the rights of others are under threat;
- the computer policy is being breached;
- laws are being broken;
- dishonest practice is occurring e.g. cheating;
- protocols or rules for the use of external systems are being broken.

Other than in exceptional circumstances, the System Administrator will undertake such non-routine action only with the prior approval of the President of LRU. In all circumstances the Head of Department and the affected user will be notified as soon as is practicable.

6.4 All users are entitled to work without harassment. The use of computer facilities to send or disseminate offensive, abusive, threatening, or unnecessarily repetitive messages or material may be considered harassment and may be subject to the University's Harassment Procedures or Discipline Regulations. For example if it is unacceptable to verbally say something to a person it is equally unacceptable to transmit the same statement electronically. Similarly, if it is unacceptable to display a sexually explicit poster in a public room then it is equally unacceptable to display such an image on a publicly visible computer screen.

6.5 Nefarious (wicked or criminal) activities include uploading, downloading, or otherwise transmitting without authority:

- trade secrets, copyrighted, trademarked, or patented materials;
- illegal information or materials;
- objectionable materials in terms of the Films, Videos, and Publications Classification Act;

- defamatory materials;
- offensive, harassing, derogatory, or discriminatory materials within the meaning of the Human Rights Act 1993 or the Harassment Act 1997;
- material about individuals which is being used for a purpose other than that for which it was collected, in breach of the Privacy Act 1993.

6.6 Normally logging into a University-owned workstation will give you authorization to all information resources that you need. However, some systems (such as Finance) will require re-authentication for technical or security reasons. These additional authentications will be kept to a minimum.

7. Email

7.1 These email guidelines are intended to ensure that use is ethical, legal, and respectful of privacy, while at the same time protecting freedom of expression, and particularly the exercise of academic freedom, in the University. This is both for the protection of individuals and for protection of the University and its reputation.

7.2 If at any time you feel that your rights as a user are being violated, or if you are aware of other users who are misusing or abusing the email and Internet facilities, please promptly report the problem. You should make this report in the first place to your immediate supervisor. Failing a satisfactory response you should then report to the manager of the computer system you were using, or to your Head of Department, or Chief Information Officer, in turn until a satisfactory response has been obtained.

7.3 Remember to prepare your email account if you will be away for some time. This may include automatic forwarding of messages to another person or account, and stopping subscriptions to distribution lists.

7.4 Your rights to your email cease when your enrollment or employment at the University ceases, though students and staff may make ongoing arrangements through the Institution itself. You should print out or make copies of any messages you wish to keep.

7.5 Message Creation-

Great care must be used in creating electronic communications because they may reflect upon the University's reputation, and in some circumstances render it legally liable, and can be intercepted.

So others cannot send email under your username, make sure that unauthorized people do not have access to your user accounts, and do not tell others your passwords.
Though they have almost the immediacy and spontaneity of a conversation, email messages are devoid of "body language". Something said verbally may be interpreted quite differently in the context of email. To avoid causing unintentional offense or misunderstanding, it is useful to read over a message before sending it and to ask yourself what your reaction would be if you received it, given its particular context. Other useful guidelines are to be concise and to provide a short but meaningful "subject".

7.6 Privacy and Ownership of Messages-

Before forwarding a message you have received, consider obtaining the consent of the author. The author may regard the message as private or sensitive in some way, and there

may be copyright implications. This is particularly true when forwarding to a distribution list, where the message may not be seen in the context it was intended.

7.7 Information Protection-

You should assume that any communication may be read by someone other than the intended recipient. Think of your email as being more like a postcard than a sealed letter. If the content is highly confidential or sensitive, convey it by another means, or encrypt it.

Email can be forged so that it appears to come from someone other than the true sender. If the authenticity of a message is crucial, you should convey it by another means, or use a digital signature or encryption.

Delivery of email messages, and delivery within a specific time, cannot be guaranteed. If your message is time critical, consider sending it by another method.
Sending or forwarding of email to the wrong person is very easily done and not very easily undone. Check carefully before sending.

You should be aware that deleting email messages from your email system does not necessarily delete all copies of those messages. For example, they may have been backed up as part of routine computer systems management.

7.8 Viruses-

Programs and documents containing macros received by email are a frequent source of computer viruses. Such files should be scanned with virus detection software before accessing or use

8. Connection of Equipment to the University Network

8.1 Failure to comply with this policy may result in the immediate termination of your campus network connection. Where practicable, warning will be given to the users before any equipment is disconnected because of being a threat to the integrity of the network.

8.2 Computers disconnected under 5.2 will not be allowed back on the network until certified by the IT Helpdesk.

8.3 Microsoft Security Essentials anti-virus software is a free download available to anyone by visiting www.microsoft.com. Any computer attaching to the LRU network must have a current version of a reputable Anti-Virus program installed and running.

8.4 User Activity-

Included in the Institution's financial liability, is all user traffic originating from and to your computer, regardless of whether or not you generated it; you know and understand the implications of what you are doing; or you realize that you have violated any specific policies.

8.5 Computer Names-

For guidelines related to naming of University-owned computers, see the Computer Administration Policy.

The name of your computer is valid only within the internal University Network and is not published on the Internet.

8.6 Interfering with Other Computers-

Interference is unacceptable no matter where the computer being interfered with is located. Interference includes share and port scanning, password-cracking, sending unrequested messages, running hacking scripts, and the like. It should be kept in mind that port scanning is considered by the vast majority of network administrators to be a "hostile" act and a precursor to a hacking attempt.

8.7 Security and Privacy-

In cases where a computer is "hacked into", it is mandatory that the system be either shut down or be removed from the campus network as soon as possible in order to localize any potential damage and to stop the attack from spreading. The IT department reserves the right to disable the network connection to isolate the compromised computer. Any computers with shared drives or directories that are password protected are considered private, even if others that do not own the computer know the password. Accessing password protected directories without the express permission of the owner is considered hacking, and may result in permanent loss of network privileges.

8.8 Personal File Sharing-

Current operating systems have options that allow personal file sharing of folders or directories on the local hard-disk. It is recommended that these shares are read-only to avoid infection by viruses.

8.9 Network Traffic and Bandwidth-

There are no restrictions on the amount of international traffic a single computer can generate. However, excess use for extended periods of time will have an impact on others and may result in disconnection.

8.10 Piracy and Copyright-

The possession of unauthorized copyrighted material, e.g. commercial MP3 music or DivX movies, on your computer is illegal. It does not matter if it is for your personal use only, it is still illegal. It does not matter if everyone is doing it, it is still illegal. The photocopying "fair use" concept does not apply to electronic digital media.

Sharing of copyrighted material through such processes as peer-to-peer file sharing like KaZaA or Limewire is strictly prohibited. It is illegal and may lead to criminal proceedings and may even implicate the University. Use of such peer-to-peer systems over the Internet may generate large amounts of unexpected Internet traffic and be compounded by excessive fees. It generates real costs to the University, for which you are held liable. Typical penalties for minor infractions are the short term suspension of networking privileges. More serious infractions may result in permanent loss of privileges, as well as further disciplinary measures that may involve contacting appropriate law enforcement.

8.11 Connection of Modems-

Information Technology is responsible for maintaining the integrity of the campus network. The connection of a device to the campus network that can be accessed directly from the wider Internet, without going through the University firewall, constitutes a potential security risk to the network. Such devices include regular analogue modems, DSL modems, ISDN modems, and any type of wireless access device. Typically this will

be a modem or wireless access device connected to a desktop computer (or server) that is itself connected to the campus network. Through these devices, hackers anywhere in the world can potentially get onto the campus network by-passing the usual University firewall logging, virus scanning of email attachments, and system security.

Related Policies, Procedures and Forms:

- Computer Crimes link
  http://www.fbi.gov/about-us/investigate/cyber
- Harassment Policy Statement and Complaints Procedures
  http://abhe.lru.edu/Documents/Manuals/2014%20Student%20Handbook.pdf
  Section 100.3, page 10
  http://abhe.lru.edu/Documents/Manuals/Faculty%20Handbook%20-%20Updated%20January%202013.pdf
  Section 100.3.4, page 29
  http://abhe.lru.edu/Documents/Manuals/Staff%20Handbook.pdf
  Sections 600.14, page 47, Section 600.25, pages 49 & 50
- Computer Administration Policy & Procedures
- Harassment Act 1997
  http://www.legislation.govt.nz/act/public/1997/0092/latest/DLM417078.html
- Privacy Policy of the University
  http://www.lru.edu/Content.aspx?page=privacy&tool=quicklinks
- Privacy Act of 1993
  http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html
- Films, Videos, and Publications Classification Act 1993
  http://www.legislation.govt.nz/act/public/1993/0094/latest/DLM312895.html
- Copyright Act
  http://www.copyright.gov/title17/

Notes:

1. For further information about these policies and procedures contact Ken Stokes at 678-990-5511.

2. Where department/school is referred to in this document, it is also intended that other organizational arrangements like colleges, service units, and centers are covered by this reference.