Technology Elevated

Computer Systems Acceptable Use Policy for Employees

Effective August 1, 2014

Purpose

This policy is designed to oversee and regulate the use of Lees-McRae College computing and communications resources and to manage and secure College data and other information assets.

Sources

Lees-McRae College, Inc. and Lees-McRae Office of Technology Services

Applicability

Faculty, Administrative (classified and College staff), academic professionals and courtesy affiliates

Introduction

Policy

This policy defines the boundaries of acceptable use of Lees-McRae College computing and communication resources, including computers, data storage systems, mobile devices, electronic data, networks, electronic mail services, electronic information sources, voice mail, telephone services, and other communication resources. In addition, this policy reflects the goal of Lees-McRae to foster academic freedom while respecting the principles of freedom of speech and the privacy rights of students, faculty, employees, courtesy affiliates and guests.

Lees-McRae's computing and communication resources are the property of the College. They are to be used for the advancement of Lees-McRae's educational, research, service, administrative, and business purposes. Computing and communication resources are provided for the use of faculty, staff, currently admitted or enrolled students, and other properly authorized users. When a user's affiliation with the College ends, Lees-McRae will terminate access to computing and communications resources and accounts. The College may, at its discretion, permit the user to have the access to accounts and email forwarded or redirected for a limited period of time.

The Office of Technology Services is responsible for the maintenance and security of the College's central computing and communications resources. This includes recommendations for effective practices by its users, which include faculty, staff, and affiliates. This policy is designed to aid the College community in protecting the confidentiality, availability, and integrity of College information resources.

All users of Lees-McRae are computing and communications resources are required to comply with this policy and state and federal laws. When necessary, enforcement will be consistent with other applicable College administrative policies and procedures.

Requirements for the Use of College Computing and Communications Resources

1. Users must comply with all applicable local, state and federal laws and regulations.
2. Users must respect academic freedom and free speech rights.
3. Users must be truthful and accurate in personal and computer identification.
4. Users must respect the rights and privacy of others, including intellectual property and personal property rights.
5. Users must not compromise the integrity of electronic networks, must avoid restricted areas, and must refrain from activities that may damage the network, or transmitted or stored data.
6. Users and individuals responsible for system administration must maintain the security of accounts and are required to protect and regularly change their account passwords.

7. Users, once aware of a security concern, must notify the Office of Technology Services of information security concerns including, but not limited to, breaches of sensitive data or compromised accounts.
8. Users are responsible for the protection, security, and integrity of College data and resources under their control.

Prohibited Uses of College Computing and Communications Resources

1. Unlawful communications, including threats of violence, obscenity, child pornography, and harassing communications, are prohibited.
2. Use of Lees-McRae computer resources for private business or commercial activities, or for fund-raising or advertising on behalf of a non-Lees-McRae organization, is prohibited.
3. The unauthorized reselling of College computer resources is prohibited.
4. Unauthorized use of College trademarks or logos and other protected trademarks and logos is prohibited.
5. The Lees-McRae web may link to commercial websites, but any link that generates, or has the potential to generate, revenue to Lees-McRae or to any individual or company, must be approved by the Business Affairs Office.
6. The Lees-McRae website may include links to commercial websites to provide information related to the mission or function of the College or academic or administrative unit. Any link that generates, or has the potential to generate, revenue to the College or academic or administrative unit must be approved through the Business Affairs office.
7. Any alteration of addresses, uniform resource locator (URL), or other action that masks the lmc.edu domain as a host site is prohibited.
8. Unauthorized anonymous and/or pseudonym communications are prohibited. All users are required to cooperate with appropriate Lees-McRae personnel or other authorized personnel when investigating the source of anonymous messages.
9. Misrepresenting or forging the identity of the sender or the source of an electronic communication is prohibited.
10. Unauthorized attempts to acquire and use passwords of others are prohibited.
11. Unauthorized use and attempts to use the computer accounts of others are prohibited.
12. Altering the content of a message originating from another person or computer with intent to deceive is prohibited.
13. Unauthorized modification or deletion of another person's files, or account postings is prohibited.
14. Use of College computer resources or electronic information without authorization or beyond one's level of authorization is prohibited.
15. Interception or attempted interception of communications by parties not authorized or intended to receive them is prohibited.
16. Making College computing resources available to individuals not affiliated with Lees-McRae without approval of the Office of Technology Services is prohibited.
17. Compromising the privacy or security of electronic information is prohibited.
18. Infringing upon the copyright, trademark, patent, or other intellectual property rights of others in computer programs or electronic information (including plagiarism and unauthorized use or reproduction) is prohibited. The unauthorized storing, copying, or use of audio files, images, graphics, computer software, data sets, bibliographic records, and other protected property is prohibited except as permitted by law.
19. Interference with or disruption of the computer or network accounts, services, or equipment of others is prohibited. No personal routers, access points, switches, non-Lees-McRae desktop computers, etc. are to be installed by non-Lees-McRae IT personnel in all campus locations.
20. The propagation of computer "worms" and "viruses," the sending of electronic chain mail, denial of service attacks and inappropriate "broadcasting" of messages to large numbers of individuals or hosts are prohibited.
21. Failure to comply with requests from appropriate Lees-McRae staff to discontinue activities that threaten the operation or integrity of computers, systems, or networks, or that otherwise violate this policy is prohibited.
22. Revealing passwords or otherwise permitting the use by others (by intent or negligence) of personal accounts for computer and network access without authorization is prohibited.
23. Altering or attempting to alter files or systems without authorization is prohibited.
24. Scanning of networks, networked devices, or applications for security vulnerabilities without specific authorization by the Office of Technology Services is prohibited.
25. Attempting to alter or connect any computing or networking components (including, but not limited to, non-Lees-McRae desktop computers, bridges, routers, DHCP servers, wireless access points, and hubs) on the Lees-McRae network without approval of the Office of Technology Services is prohibited.
26. Installation or alteration of wiring, including attempts to create network connections, or any extension or retransmission of any computer or network services without the approval of the Office of Technology Services is prohibited.
27. Conduct leading to disruption of electronic networks or information systems is prohibited.
28. Conduct leading to the damage of College electronic information/data, computing/networking equipment, and resources is prohibited.

Information Posted to College Computers or Web Pages

Restriction on Use of College Web Pages

College web pages may be used only for Lees-McRae business and only authorized individuals may modify or post materials to these pages. No other pages may suggest that they are College web pages. If confusion is possible, pages should contain a disclaimer and links to Lees-McRae sites.

Responsibilities of Individuals Posting Materials

By posting materials and using College computing facilities, the user represents that he or she has created the materials or that he or she has the right to post or use the materials. The storage, posting, or transmission of materials must not violate the rights of any third person in the materials, including copyright, trademark, patent, trade secrets and any rights of publicity or privacy of any person. The materials posted must not be defamatory, libelous, slanderous, or obscene.

Prohibition against Commercial Use

The site may not be used for unauthorized commercial purposes.

Control of College Web Pages

The use of the site is at the sole discretion of Lees-McRae. The College does not guarantee that the user will have continued or uninterrupted access to the site. The site may be removed or discontinued at any time at the discretion of Lees-McRae in accordance with College policy, or as needed to maintain the continued operation or integrity of College facilities.

Lees-McRae makes reasonable efforts to protect the integrity of the network and related services, but cannot guarantee backup, disaster recovery, or user access to information posted on personal computers or web pages.

Access to services and file storage may be approved for emeriti, retired staff, alumni, and guests.

Restrictions on the College Network

Lees-McRae College reserves the right to restrict certain web content when it is deemed illegal or could constitute copyright abuse. The use of any P2P software (Limewire, KaZaa, the Pirate Bay, etc.) is strictly prohibited on the Lees-McRae network due to copyright abuse. However, there are several alternatives to P2P that are legal. The following sites and/or programs can be used to obtain legal media such as music, movies, books, etc.

Music	Movies	Books	Software
YouTube	YouTube	Audible	CNet
Grooveshark	Netflix	Amazon	
iTunes	HBO Go	Barnes and Noble	
Pandora	RedBox	eBooks.com	
Last.fm	Hulu		
Slacker Radio	CinemaNow		

For more information on legal alternatives for downloading, please refer to the website Educause Legal Alternatives. If you encounter a website, particularly one related to academic research, that you believe has been unjustly limited, or if you have any other concerns related to internet access, please submit a ticket to Technology Services via the HelpDesk.

Electronic Mail and Electronic Communications

Conditions for Restriction of Access to Electronic Mail

Access to Lees-McRae email is a privilege that may be wholly or partially restricted without prior notice and without consent of the user:

1. if required by applicable law or policy;
2. if a reasonable suspicion exists that there has been or may be a violation of law, regulation, or policy, or

3. if required to protect the integrity or operation of the email system or computing resources or when the resources are required for more critical tasks as determined by appropriate management authority.

Access to the email system may require approval of the Office of Technology Services.

Conditions for Permitting Inspection, Monitoring, or Disclosure

Lees-McRae may permit the inspection, monitoring, or disclosure of email, computer files, and network transmissions when:

1. required or permitted by law, including public records law, or by subpoena or court order;
2. Lees-McRae or its designated agent reasonably believes that a violation of law or policy has occurred or,
3. as necessary to monitor and preserve the functioning and integrity of the email system or computer systems or facilities.

All computer users agree to cooperate and comply with College requests for access to and copies of email messages or data when access or disclosure is authorized by this policy or required or allowed by law or other applicable policies.

College Responsibility to Inform of Unauthorized Access or Disclosure

If Lees-McRae believes unauthorized access to or disclosure of information has occurred or will occur, the College will make reasonable efforts to inform the affected computer account holder, except when notification is impractical or when notification would be detrimental to an investigation of a violation of law or policy.

Prohibition against Activities Placing Strain on Facilities

Activities that may strain the email or network facilities more than can be reasonably expected are in violation of this policy. These activities include, but are not limited to: sending chain letters; “spam,” or the widespread dissemination of unsolicited email; and “letter bombs” to resend the same email repeatedly to one or more recipients.

Confidentiality

Confidentiality of email and other network transmissions cannot be assured. Therefore all users should exercise caution when sending personal, financial, confidential, or sensitive information by email or over the network.

Electronic Information as North Carolina Public Record

Most electronic information (e.g., email) produced in the course of College business is considered an North Carolina public record (http://www.sog.unc.edu/sites/www.sog.unc.edu/files/public_records_overview.pdf), and must be stored or deleted in accordance with North Carolina Public Record Law. Consult with the Office of Technology Services for guidance on procedures for external storage or deletion of public records.

Privacy and Security

Routine Logging and Monitoring

Certain central service and network activities from workstations connected to the network are routinely logged and monitored. These activities include but are not limited to:

1. use of passwords and accounts accessed,
2. time and duration of network activity,
3. access to web pages,
4. access to network software, and
5. volume of data storage and transfers and server space used for email.

Responsibility for Data Security

Software and physical limitations, computer viruses, and third-party intrusions can compromise security of data storage and communications. Lees-McRae takes reasonable precautions to minimize risk. Users must notify the Office of Technology Services when there is a breach of sensitive data or compromised accounts.

Individual users and departments should develop policies and practices, coordinated with Office of Technology Services as needed, to ensure regular backups of data and to implement steps to ensure that all critical data is compatible with all current generations of computing equipment, storage media, and media readers.

Restriction of Access to Sensitive Data

All Lees-McRae departments should ensure that access to sensitive data is restricted to those employees who have a need to access the information. Passwords that provide access to sensitive information should be changed on a regular basis.

Right to Examine Computers and Equipment

College-owned computers and equipment may be examined to detect illegal content and to evaluate the security of the network. Networks, networked devices, and applications may be scanned for vulnerabilities as authorized by the Office of Technology Services.

Violations and Enforcement

Reporting Violations

Any actual or suspected violation of the rules listed above should be brought to the attention of the Office of Technology Services.

College Response to a Reported Violation

Upon receiving notice of a violation, Lees-McRae may temporarily suspend a user's privileges or move or delete the allegedly offending material pending further proceedings.

A person accused of a violation will be notified and have an opportunity to respond before the College imposes a permanent sanction. Appropriate cases will be referred to the Lees-McRae authority appropriate to the violator's status (e.g., Human Resources or the President) or to appropriate law enforcement authorities.

In addition to sanctions available under applicable law and College policies, Lees-McRae may impose a temporary or permanent reduction or elimination of access privileges to computing and communication accounts, networks, College-administered computing rooms, and other services or facilities.

If Lees-McRae believes it necessary to preserve the integrity of facilities, user services, or data, it may temporarily suspend any account, whether or not the account user is suspected of any violation. Lees-McRae will provide appropriate notice to the account user. Servers and computers that threaten the security of College systems will be removed from the network and allowed to reconnect only with the approval of Office of Technology Services.

Distribution of this Policy

The College will ensure that all users are aware of the policy by publishing it in appropriate media designed to reach all faculty and staff.