Acceptable Use Policy at Lourdes University

Purpose

As part of its educational mission, Lourdes University acquires, develops, and supports technology resources for students, faculty, staff, and the supporting community. This technology is intended for University-related purposes, including direct and indirect support of the University's teaching, scholarship, and service missions; University administrative functions; student and campus life activities; and the free exchange of ideas within the University community. This policy governs the use of information technology systems and electronic resources at Lourdes University.

The Acceptable Use Policy for Information Technology at Lourdes University promotes the efficient, ethical, and lawful use of the University's information technology resources. The University's computing systems, networks, and associated facilities are intended to support its mission and to enhance the educational environment. Any use of these resources deemed inconsistent with the mission and purpose of the University will be considered a violation of this policy.

Policy Statement

This policy shall be applicable to all students, staff, faculty, and contractors/vendors (defined hereafter as 'users') who have access to or who are responsible for any University system account at any University facility. This policy also applies to anyone who has access to the University network, who stores electronically any non-public information elsewhere, or who use a University-owned desktop, laptop or tablet computer., or other electronic device. By using the University's information technology resources, all users agree to the rules, regulations, and guidelines contained in this Acceptable Use Policy.

Information technology systems and electronic resources are provided to the members of the University community with the understanding that they will use them with mutual respect, cooperation, and collaboration, and in compliance with all applicable policies, laws, and regulations.

Information technology resources are finite, but their usage is growing and expanding; the resources must be shared generally and as with any interconnection of electronic resources, one individual can have a dramatic effect on others within the network. Therefore, the use of the network and electronic resources is a revocable privilege.

All constituents will benefit if all users of the electronic systems avoid any activities that cause problems for other users. The University reserves the rights to monitor, limit, and restrict electronic messages, network/systems traffic, and the public or private information stored on computers owned, maintained, or managed by the University. Anyone who uses computers not owned, maintained, or managed by the University that abuse campus services may also be denied access to campus resources. Email/voice mail, web pages, and digital content are subject to archiving, monitoring, or review, and/or disclosure by those other than the intended recipient.

Technology Systems and Electronic Resources

The University requires access to its information technology systems and electronic resources (hereinafter "Systems") to be authorized and pre-approved, and that users understand that laws currently exist that prohibit the following:

1. Electronic libeling or defamation
2. Sending/posting/broadcasting messages that incite hate or violence
3. Transmitting repeated unwanted personal advances
4. Falsifying information or impersonation
5. Unauthorized use of, providing, or copying of protected intellectual or copyrighted property

University Network

The University network is a private network separate and distinct from the public internet. Therefore, access to and use of this network must comply with all University policies, rules, and regulations, and with all local, state, and federal laws. Examples of prohibited activities outside of prescribed course or business-related activities include but are not limited to:

1. Posting or transmission of confidential information
2. Use of offensive or discriminatory language
3. Transmission or display of graphic images, sounds or text that is sexual or offensive in nature
4. Use of other users' passwords or accounts
5. Use of the Systems for personal profit or gain
6. Use of the Systems to harass, threaten, or otherwise invade the privacy of others
7. The installation or use of any servers on the network not expressly approved by Information Technology Services
8. Deliberate attempts to cause breaches of the network, servers, telecommunications systems, or security or to examine network traffic
9. Initiation of activities that unduly consume computing or network resources
10. Use of applications, for example, P2P, to receive and/or distribute copyrighted materials, such as movies, music, and video
11. Tampering with computer files, software, or knowingly introducing a virus or malicious code to the University systems
12. Unauthorized changes to University web pages
13. Playing games in computer labs for entertainment
14. Excessive use of network bandwidth, storage, and any computer resources for purposes unrelated to University activities
15. Unauthorized access of University resources and/or data

Lourdes University expects users to access and use the University's electronic information and information systems in a manner that:

1. Does not compromise the confidentiality, integrity, or availability of those assets
2. Reflects the University's standards as defined in this policy

University Owned Tablet Devices, Including iPads Provided Through the iWolf Program

iPads by design are single-user devices that are not intended to be shared among several users and must maintain information security and privacy in the University environment. Departments purchasing iPads, including those purchased for student use through the iWolf program, must be assigned to one person for individual use. In the case whereby such a device is intended to support specific, targeted purposes by groups of individuals, no personal information may be stored on the device. All devices registered for check-out purposes must be fully reset and information wiped before assigning to another individual.

Provisions for Private Devices Connected to the University Network

The following applies to anyone connecting a private device (computer, tablet, phone, gaming system, or other similar device) to the University network via the University housing network, a wireless LAN connection, a regular network connection in an office, or any other network connection. The owner of the device is responsible for the behavior of all users on the device, and all network traffic to and from the device, whether or not the owner is aware of the traffic generated. A private device connected to the network may not be used to provide network access for anyone who is not authorized to use the University systems. The private device may not be used as a router or bridge between the University network and external networks, such as those of an Internet Service Provider (ISP). Should Information Technology staff have any reason to believe that a private device connected to the University network is using the resources inappropriately, network traffic to and from that device may be monitored. If justified, the system will be disconnected from the network, and action will be taken by the appropriate authorities.

Any residential student with an authorized network account may use the in-room connection for scholarly purposes, for official University business, and for personal use, so long as the usage (1) does not violate any law or regulation; (2) does not involve extraordinarily high utilization of University resources or substantially interfere with the performance of the University network; (3) does not result in commercial gain or profit; and (4) is not in violation of any part of this policy.

Users are responsible for the security and integrity of their systems. In cases where a device is compromised, the user shall either shut down the system or remove it from the campus network as soon as possible to localize any potential damage and to stop the attack from spreading. Users suspecting electronic intrusion or hacking of a personal device who would like assistance should contact the IT Helpdesk immediately.

Personal servers and network equipment will never be connected to the University network without prior authorization from Information Technology.

Passwords

Passwords are an important aspect of information security. They are the front line of protection for user accounts and system integrity. A poorly chosen password can result in the compromise of the University's entire network.

A password authenticates the holder as an authorized user of the University's computer system that uses the institution's Active Directory for authentication, authorization, and auditing, and must be protected from disclosure to others. Each user is responsible for the security of their password(s). Passwords must not be shared with others and may only be used by the person for whom the password was created. Therefore, a password may not be posted in a place accessible by others and must not be inserted into email messages or other forms of electronic communication.

User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user. Group passwords are allowed only in the case of the

highest-level administrator passwords for servers and should not be used for the day-to-day administration of the system.

Active Directory Password Construction

Users must select passwords that comply with the University's stated password procedures. Simple or weak passwords must not be used. Simple or weak passwords have the following characteristics:

1. The password contains less than eight characters.
2. The password is a word found in a dictionary (English or foreign).
3. The password is a common usage word such as names of family, pets, friends, co-workers, fantasy characters, etc.
4. Computer terms and names, commands, sites, companies, hardware, software.
5. Birthdays and other personal information such as address and phone number.
6. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
7. Any of the above spelled backwards.
8. Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Active Directory Password Changes

All user-level passwords (e.g., network, domain, email, desktop computer, etc.) must be changed at least once a year.

Contractor accounts will automatically expire 180 days after creation unless there is an exception is approved by the Chief Information Officer.

User-level passwords must be unique for 10 consecutive password changes, i.e., a password cannot be reused for 10 password changes.

Passwords must meet with complexity requirements stated above.

Accounts will be locked after five consecutive unsuccessful login attempts for 30 minutes or until an administrator enables the user ID.

All users will receive an automated notification, when logging in to a University computer or service, notifying them their password will expire. If the current password is not changed before it expires, a password change will be prompted upon the user's first login attempt after the expiration date and the user will not be able to log in to the University network until the password is changed.

Generic Accounts/Non-repudiation

Generic network accounts prevent the University from maintaining personal accountability and prevents the implementation of proper internal controls to safeguard University systems and data assets. Any account created that may allow multiple users to use a single account to log on to network resources is considered a generic account. While generic account use is not permitted, Information Technology Services will work with departments to minimize impact on business operations where common accounts (e.g., email) are required for business operations to meet business requirements, but uphold necessary security requirements, such as through account delegation.

Muti-Factor Authentication

All user accounts, including those for student, staff, faculty, and contractor use, must utilize Multi-Factor Authentication (MFA). MFA is a method of authentication that requires more than one verification method, commonly relying on something a user knows (e.g., a password) and something a user has (e.g., a phone or hardware token). For service accounts, such as those running background services, other methods of MFA will be used, such as password and certificate.

Email

Users must understand that email is not absolutely private and should practice caution in sending messages that a user would not want everyone to see. It should be understood that email is not a secure communications platform. Protected information and sensitive data must not be sent through this means. Information Technology does not make a practice of monitoring email and other files; however, when there is a reasonable suspicion of wrongdoing or computer misconduct, the University reserves the right to examine material stored on or transmitted through its Systems.

VPN Access

Virtual Private Network (VPN) access is intended for use of authorized members of the community to support their work when not physically located on the Lourdes University campus. VPN access is controlled using ID and password authentication. Only authorized staff using University-owned and maintained equipment may utilize VPN services.

Intellectual Property and Copyright Protection

The University and users of its Systems must comply with the copyright protection given by international agreements and federal law to owners of software and intellectual property under the United States copyright laws, including but not limited to the Copyright Act of 1976 and the Federal Digital Millennium Copyright Act of 1998, and including the restrictions that apply to the reproduction of software and intellectual property. Users of the Systems must ensure that the bounds of permissible copying under the fair use doctrine are not exceeded (i.e., a backup copy may be made). It is against the law to copy or reproduce any licensed software or intellectual property, or to download from the Internet any copyrighted material, including, but not limited to, music, movies, and videos without the permission of the copyright holder. No one may use software that has been obtained illegally on the University's Systems or on personal equipment. Violation of these requirements will subject the offender to disciplinary action as outlined below, as well as expose the user to accountability in a court of law.

Phones and Related Systems

Lourdes University telephones, telephone lines, and fax machines are available for faculty and staff members and student employees to use in carrying out official business of the University. The placing and receiving of phone calls from Lourdes University-provided phones or faxes for reasons other than official Lourdes University business should be very infrequent and are permissible only if proper supervisory approval is granted. Faculty and staff should make every effort to minimize receiving calls or fax messages unrelated to Lourdes University business while at work.

Faculty and staff members may need to occasionally use Lourdes University telephones, telephone lines, and fax machines for personal reasons. Normally, such use should not result in additional costs or not hinder the day-to-day operation of the University. Incidental use of such equipment is permissible so long as it does not unduly interfere with the individual's assigned responsibilities or the normal functioning of the University operations.

Long-distance calls and faxes include any call that is not local or free of charge to Lourdes University. In instances where it is necessary to place a personal long-distance call over a Lourdes University phone, a personal phone telephone credit card must be used, the call must be collect or charged to a third party. Occasionally, a personal long-distance call or fax may occur by accident or may be necessary in the case of a personal emergency. When such a situation arises, the call(s) must be reimbursed promptly through the University Finance Department.

Equipment Usage

While computer equipment and access to Systems are provided for work and education purposes, incidental personal use is permitted as long as it is not inconsistent with this Policy and it doesn't interfere with employment and education responsibilities.

Software and Related Systems

All IT purchases, hardware or software, must be reviewed and approved by information technology prior to purchase, regardless of funding source. Computer software is provided for use on University-owned equipment through campus agreements managed by ITS or other departments. Funding is provided either centrally or by cost sharing among the departments utilizing the software. Software from these campus agreements must only be installed on University-owned computers.

To avoid duplication of administrative data and/or systems, to ensure data and network compatibility and to ensure that the software can be supported, software that uses or interfaces to institutional data (or potentially could interface) must be approved by the Chief Information Officer prior to purchase or development. Institutional data includes data involved in the official operation of University functions including those at the department or school level. Additionally, any software involved in payment processing must meet the finance office requirements, including receiving the approval by the Chief Information Officer and Chief Finance Officer before being purchased or implemented.

Violation, Remediation, and Intervention

Any suspicion of a password being compromised on a system that uses the University's Active Directory for authentication, authorization, and auditing must be promptly reported to Information Technology. Active Directory accounts suspected of being compromised or misused will be disabled by IT. IT will disable Active Directory accounts promptly at the notice of termination by the Human Resources department. The University may also impose restrictions pertaining to computer use, including a loss of computing privileges on a temporary or permanent basis, a decrease of disk quota, and the removal of files in the System's temporary or scratch area.

In addition to liability and penalties that may be imposed under federal, state, or local laws, users of the Systems who fail to fulfill their responsibilities and engage in prohibited conduct may be subject to disciplinary action. The University may restrict or suspend user privileges while the alleged violation(s) are being investigated and disciplinary action pursued. Disciplinary action may be taken by the appropriate officer relative to student, faculty, staff, and/or affiliate violations. A violation may also result in a referral to law enforcement authorities.

In accordance with the University's policies and state and federal laws, IT may monitor the University network for activity that violates this Acceptable Use Policy.

Disclaimers

The President of the University and Chief Information Officer have the discretion to suspend or rescind all or any part of this policy or related procedure(s). The President or Chief Information Officer shall notify appropriate personnel of the suspension or rescission.

The University makes no warranties of any kind, either express or implied, for the Internet services it provides. The University will not be responsible for any damages suffered by users, including, but not limited to, any loss of data resulting from delays, non-deliveries, user errors, or service interruptions.

The University is not responsible for the accuracy or quality of information obtained through its internet services, including e-mail. Users assume responsibility for any damages suffered due to information obtained through these sources.

The user agrees to indemnify and hold harmless the University, the board of trustees, and University employees and contractors from and against any claim, lawsuit, cause of action, damage judgment, loss, expense, or liability resulting from any claim, including reasonable attorneys' fees, arising out of or related to the use of the University's hardware, software, and network facilities. This indemnity shall include, without limitation, those claims based on trademark or service mark infringement, trade name infringement, copyright infringement, defamation, unlawful discrimination or harassment, rights of publicity, and invasion of privacy.

Approved

May 3, 2022, by the President's Cabinet of Lourdes University.

MDM 5/3/2022