TECHNOLOGY ACCEPTABLE USE POLICY (AUP)

AA-IT-PO-001

POLICY OVERVIEW

Our Lady of the Lake University makes available to its community members computing and network resources, including shared information technology resources that use text, voice, images, and video to deliver information. These resources are to be used in a responsible manner consistent with the University's mission and core values, other University policies, state and federal laws and regulations, and applicable OLLU information security policies and standards.

POLICY SCOPE

WHO: The Technology Acceptable Use Policy ("AUP") applies to all active members of the University community (including faculty, students, staff, alumni, and affiliates) and to authorized guests, and others for whom University technology resources and network access are made available by the University. This includes campus visitors who avail themselves of the University's temporary visitor wireless network access service.

WHAT: This policy applies to University-owned devices and systems and to University-contracted systems and services, as well as privately-owned or publicly-provided devices using the University's networks, or storing and/or transmitting University data; to technology administered by individual departments or members of the faculty or staff or by campus organizations; and to

personally-owned devices connected by wired or wireless service to the campus network, from University-owned housing, or via campus locations providing mobile wireless access. It also applies to websites bearing the University credentials, even when hosted outside the University's Internet domain.

POLICY

1. TECHNOLOGY ACCEPTABLE USE

A. INSTITUTIONAL USE

Use of all University information technology and digital resources should be for purposes that are consistent with the non-profit educational mission and the policies and legal requirements (including license agreements and terms of service) of the University.

B. PERSONAL USE

Personal use of the University's information technology and digital resources, except for students enrolled at the University, should be incidental and kept to a minimum.

C. PROHIBITED USE

Use of the University's information technology and digital resources should not violate applicable federal, state, and local law, including U. S. copyright law, or applicable University policies, and, if travel is involved, the laws of the relevant nation or state. From any location, University resources may not be used to transmit malicious, harassing or defamatory content.

Members of the University community are prohibited from using University information technology and digital resources for commercial purposes.

Individuals may not use University technological resources for political purposes in a manner that suggests the University itself is participating in campaign or political activity or fundraising, or for influencing legislation.

2. ACCESS AND PRIVACY

In general, and subject to applicable law, the University reserves the right to access, copy and/or destroy information (including e-mail, voice messages, and text messages) residing on University-owned devices and other technology systems, and in storage contracted by the University from outside enterprises. The University also reserves the right to access, copy and/or destroy

University information on personally-owned devices if the devices are used to conduct University business. This includes access without notice, where justified by the University's operational and/or legal needs and consistent with applicable laws.

Students, for whom the University effectively is a residence during the academic year, normally are afforded a high degree of privacy. University employees are afforded a lesser degree of privacy with respect to business-related systems and information. In the event that business-related information or files (including e-mail, digitized voice messages and text messages) must be accessed based on business need or where required by law, they may be accessed by the University after consultation with the appropriate University offices (e.g. Office of the Provost and Vice President for Academic Affairs, Office of the Vice President for Student Life, Office of the Vice President for Administration).

3. PROTECTION OF UNIVERSITY RESOURCES

Users of University information technology and digital resources are responsible for protecting University data, including its confidentiality, integrity, access, retention and disposal, in accordance with the University's information security program, record retention policy, and other applicable University policies. Individuals with University accounts or administrative responsibility over any University resources should take reasonable measures to protect these accounts and resources. Shared University technological resources should be used for educational purposes and to carry out the legitimate business of the University, and should not be used in a way that disrupts or otherwise interferes with any University activities or systems or that is inconsistent with the University's policies or goals.

4. VIOLATIONS AND PENALTIES

Violations of the policy may result in disciplinary action, including termination from employment, expulsion, or suspension of network privileges.

REFERENCES

- Guidelines for Compliance with the Technology Acceptable Use Policy
- Information Security Policies
- OLLU Information Security Program
- Mobile Device Policy
- Social Media Guidelines