SAGRADO
Universidad del Sagrado Corazón

Policy on the Use of Technology and Information Resources

Effective: July 1, 2019

Purpose

Sagrado (also known as "the University") provides access to information technology ("IT") resources and communication networks within a culture of openness, trust, and integrity. Furthermore, the University is committed to protecting itself and its students, faculty, and staff from unethical, illegal, or harmful actions by individuals who use these systems.
Unless otherwise specified in this policy or other University policies, the use of the University's computing resources is restricted to purposes related to the University's mission.

Users of the Sagrado network and computing resources ("users") are responsible for the proper use and protection of information resources. This Policy covers the appropriate use of all information resources, including computers, networks, and the information contained therein.

Scope

This Policy applies to all university students, full-time and part-time faculty, administrative and contract employees, and any entity granted access to and use of Sagrado's IT resources.

Definitions

Information and technology resources include all computing and communication devices and other technologies that access, store, or transmit university or student information.

Information includes data or references pertaining to the University and students.

Privately owned resources are information resources that are under the control of university employees or agents and are not the exclusive property of the university.

General Policy

It is the responsibility of both those who administer the systems and those who use them to secure and protect IT resources from misuse or malicious activity.

Users of information resources must protect (a) their online identity from being used by another person, (b) the integrity of information resources, and (c) the privacy of electronic information. In addition, users must refrain from seeking or obtaining unauthorized access, respect all copyrights and licenses, and respect the rights of other users of information resources.

Access

Eligible individuals are provided access to support their studies, instruction, employee duties, official business with the University, and other University activities. Individuals may not share or transfer their University accounts to others, including network IDs, passwords, or other access codes that allow them to access University accounts, including network IDs, passwords, or other access codes that allow them to access the University's IT resources.

Users must refrain from attempting to gain unauthorized access to IT resources or facilitating unauthorized access. Attempts to gain unauthorized access to a system or another person's information constitute a violation of University policy and may also violate applicable law, which may expose the user to civil and criminal liability. However, authorized system administrators may access IT resources, but only for legitimate operational purposes and only with the minimum access required to achieve that legitimate operational purpose.

1. Sharing Credentials Is Prohibited

Sharing an online credential (username and password or other identifier such as *a token* or certificate) violates University policy

2. Information Belonging to Others

Users must not provide information, obtain copies of, or modify data files, programs, passwords, or other digital materials belonging to other users.

3. Abuse of IT Privileges

Users of IT resources must not access computers, software, data, or information on computers or networks without proper authorization, or intentionally allow others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the University. For example, misuse of networks owned by the University or of computers at other locations connected to those networks will be treated as a violation of the University's computing privileges.

Use

The University is a nonprofit, tax-exempt organization and, as such, is subject to specific federal, state, and local laws regarding sources of revenue, political activities, use of property, and similar matters. It is also a contractor with the government and other entities and, therefore, must ensure the proper use of property under its control and the allocation of overhead and similar expenses. The use of the University's information resources must comply with the University's policies and legal obligations (including licenses and contracts) and all federal, local, and state laws.

1. Prohibited Use

Users must not send, view, or download fraudulent, harassing, obscene (i.e., pornographic), threatening, or other messages or material that violate applicable law or University policy. In particular, creating a hostile academic or work environment is prohibited.

2. Copyright and Licenses

Users may not use the University's facilities or networks to infringe upon the ethical and legal rights of any person or company protected by copyright, trade secret, patent, or other intellectual property rights, or similar laws or regulations. The U.S. Copyright Act prohibits the duplication, distribution, or installation of copyrighted software unless a license agreement specifically permits such actions. Users must comply with copyright laws and all software license agreements, under which software may be copied only in accordance with the terms of those agreements. For the avoidance of doubt, the illegal sharing of files using the University's information resources constitutes a violation of this policy.

- *Copying licensed software / open-source software*. Software licensed to run on a specific computer or at a particular location must not be

be copied to another computer or another location without written authorization from the vendor (for example, when specifically permitted by the vendor's written software license agreement). In general, open-source software titles are governed by a software license agreement that limits how the software may be used, modified, or distributed.

- *Unauthorized software*. Unauthorized copied software, software downloaded from an unauthorized source, or unauthorized shareware/freeware may not be installed and/or used on the University's network, computers, or other information resources.

- *Independently Purchased Software*. It is the responsibility of users to read, understand, and comply with the terms of any software license agreement for independently purchased software (including individually packaged software purchased through such outlets or directly from a vendor's website).

- *Centrally Distributed Software*. When the University provides software at no cost for the University's commercial use, the University must instruct users on how to comply with the essential terms of the license or contract, including any general limitations imposed on the use of the software. This instruction will take the form of guidance from the University's support provider that distributes or installs the software, or through notifications on the website or file share where the software is provided.

- Sagrado shall only install the software initially or as a license renewal for subscription-based software when a valid license proof is available. The presence of a particular software title on a User's previous system, possession of the installation media, installation source files, or the software license code may not entitle the User to have that software title installed on a new or replacement computer. Sagrado will not distribute software license codes in violation of the University's contracts and license agreements. The installation of software on a Sagrado computer must be performed by personnel designated by the Office of Integrated Information and Technology ("ITI").

3. Social Media communication

Users must respect the purpose of and comply with the terms of use for online media forums, including social media websites, mailing lists, chat rooms, and blogs.

4. Personal Use

IT resources may only be used for activities related to University functions that are aligned with the University's mission, values, and all applicable University policies. Under no circumstances may the use of IT resources violate the law, interfere with the fulfillment of a University employee's responsibilities, or adversely impact or conflict with activities that support Sagrado's mission.

5. Non-Priority Excessive Use of IT Resources

Priority for the use of IT resources is given to activities related to the University's mission of teaching, learning, and research. Users may be required to cease or restrict non-priority use of IT resources, such as recreational and non-academic activities.

6. Use of University Information

Users must comply with applicable data transmission and storage policies, including the Information Security Policy.

Privately Owned Resources

Sagrado does not require staff to use their personal resources to conduct University business. Individual units within the University may permit such use, and users may choose to use their own resources accordingly. Any privately owned resource used for University business is subject to this policy and must comply with all Sagrado requirements related to that type of resource and the type of data involved. Resources must also comply with additional requirements (including security controls for encryption, patching, and backup) specific to the particular University functions for which they are used.

Integrity of Information and Technology Resources

Users must respect the integrity of information and information resources.

1. Modification or Deletion of Information or IT Resources

Unless properly authorized, users must not attempt to modify or delete information or IT resources owned or used by others.

2. Other Prohibited Activities

Users must not disrupt or interfere with access to or use of the University's information or IT resources. Furthermore, users must not engage in other activities that damage, vandalize, or otherwise compromise the integrity of the University's information or IT resources.

3. Academic Research

The University recognizes the value of legitimate research projects undertaken by faculty and students under faculty supervision. The University may restrict such activities in order to protect individual and University information and IT resources, but in doing so will take legitimate academic activities into account.

Access in Connection with Legal and University Proceedings

In certain circumstances, as a result of investigations, subpoenas, or lawsuits, the law may require the University to provide electronic or other records, or information related to such records or to the use of information resources ("IT records"), to third parties. In addition, the University may, at its reasonable discretion, review IT records—including, but not limited to, those pertaining to the proper functioning of the University—in connection with investigations or audits, or to protect the safety of individuals or the Sagrado community. The University may also grant reasonable access to data to external service providers for the purpose of providing, maintaining, or improving services to the University. Therefore, users of the University's IT resources have no expectation of privacy when using the University's IT resources.

Oversight of Information Resources

The Chief Information Officer (CIO) is responsible for the management and operation of IT resources and is also responsible for ensuring compliance with all University policies related to the use and operation of IT resources. The CIO may designate another person to manage and operate the system, but responsibility for the IT resources remains with him or her. This designee is the "system administrator," who is responsible for managing and operating the IT resources in accordance with University policies, which include, among other things, access to the IT resources necessary to maintain system operations.

The system administrator must:

- take all appropriate measures to protect the security of information and IT resources
- take precautions against theft or damage to IT resources

- faithfully comply with all license agreements applicable to IT resources
- communicate this policy and other applicable policies regarding the use, security, and privacy of information
- cooperate with ITI to identify and correct problems caused by the use of the system.

The system administrator may temporarily suspend access to IT resources if necessary or appropriate to maintain the integrity of the IT resources.

Reporting Misuse of IT Resources

Users are responsible for reporting suspected misuse of IT resources—including, but not limited to, suspected illegal or inappropriate activities—to the Chief Information Officer at 787.728.1515, ext. 3571, or by email atluis.gotelli@sagrado.edu .

Inspection and monitoring of IT information and resources may be necessary to comply with this policy, conduct investigations or audits, ensure the safety of an individual or the University, comply with the law, or ensure the proper functioning of IT resources. Only the CIO (or designee) may authorize such inspection and monitoring.

Users of IT resources are expected to cooperate with any investigation into policy violations. Failure to cooperate may result in the revocation of access privileges or other disciplinary action.

Inquiries Regarding This Policy

Inquiries regarding the scope and interpretation of this Policy should be directed to the Chief Information Officer at 787.728.1515, ext. 3571, or by email atluis.gotelli@sagrado.edu .

Reports of Policy Violations

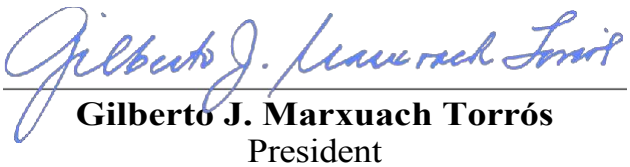
Violations of this Policy should be reported to the General Counsel at 787.728.1515, ext. 1221, or by email atcameliac.fernandez@sagrado.edu , or to the Compliance and Integrity Officer.

Violations of This Policy

La Universidad del Sagrado Corazón reserves the right to interpret this Policy in its administration, implementation, and enforcement. Any violation of this Policy by a student, faculty member, staff member, or any other person may result in disciplinary action, which may include expulsion from the University (students)

or termination of employment (faculty and administrative staff) or other appropriate legal actions.

If there is any ambiguity in any provision of this Policy, the University reserves the discretion to interpret it in accordance with the purpose for which it was established, the impact on the University's operations, and good faith, unless otherwise provided by law.



Gilberto J. Marxuach Torrós
President