Responsible Use of University Technology Resources

Regis University technology resources are to be used to advance the University’s mission of education, scholarship and service. Faculty, students and staff may use these resources for purposes related to their studies or research, their teaching, the execution of their duties as University employees, their official business with or for the University, or other University-sanctioned activities. The University encourages the use of technology resources for these primary activities. These resources include, but are not limited to, hardware (including telephones, computers, and traditional media equipment) either owned or leased by the University, software, and consulting time (and expertise) of the staff of Information Technology Services or other University technology support staff. Unless approved in advance by a vice-president or dean, use of University technology resources for commercial purposes is prohibited.

The use of technology resources provided by the University for purposes not directly related to the primary activities indicated in the previous paragraph should be considered as secondary activities (i.e. personal or otherwise.) Should such secondary activity interfere with primary activities, the University may require the immediate termination of such secondary activities.

All computer files, documents, and software created or stored on the University’s computer systems are subject to review and inspection at any time.

Many of the University’s technology resources are shared amongst the entire University community. The use of these may not violate law or the rights of others. Prohibited activities include, but are not limited to:

- Activities that obstruct usage or deny access to technology resources
- Activities that are harassing or libelous
- Activities that are obscene as applied in the context of an academic environment
- Activities that violate copyright or other intellectual property rights of others
- Activities that violate Regis University policies
- Activities that violate local, state or federal laws
- Unauthorized use of computer accounts
- Impersonating other individuals
- Attempts to explore or exploit security provisions, either at the University or elsewhere
- Activities that invade the right to privacy of others
- Destruction or alteration of data belonging to others
- Creating, using or distributing computer viruses
- Allowing other individuals to use your account/password
- Disruption or unauthorized monitoring of electronic communications or of computer accounts
- Academic dishonesty (e.g., plagiarism, cheating)
- Inappropriate and/or widespread distribution of electronic communications (e.g. “spamming”)

Additionally, individuals may wish to use University Wide Information Systems including, but not limited to, the World Wide Web, the Internet, RegisNET, and e-mail. Any person providing information through these resources or via connections to the data or telecommunications infrastructure must also abide by the general policy statements below. These policy statements apply to information made available actively, as in e-mail, as well as passively, as in the World Wide Web.

- Anonymous information is strictly prohibited. All publications must contain the electronic mail address of the person making the information available. For example, active information such as e-mail must contain the e-mail address of the sender in the FROM: field. Passive information, such as that found on the World Wide Web, must contain the e-mail address of the author, owner or sponsor at the bottom of the page.
- All information must carry a date indicating the date the information is being made available. For information made available actively, such as through e-mail, the date would appear in the DATE: field. For passive information, such as that found on the World Wide Web, the date should appear at the bottom of the page labeled as the posting date.
- Specific and detailed guidelines for the responsible use of E-mail (active) and World Wide Web (passive) technology resources exist in other policy documents. Copies can be obtained from these policy pages by returning to the Policy index page.
Members of the University community often access confidential, private or sensitive data and/or information in order to complete job responsibilities. As stewards of data and information resources, members of the University community have fundamental responsibilities, including:

- Protection of data and information from unauthorized access, alteration, disclosure or destruction.
- Secure storage of private or confidential data and information.
- Interpretation of data and information based on a job-related "need to know."
- Presentation of data and information based on the audience's authorized "need to know."
- Disposal of confidential data and information, particularly that which is redundant, when the purpose for use has been met.

The University intends to place effort toward development of technology resources and not the policing of the use of those resources. Engaging in activity that violates or is prohibited by current faculty, student, and staff operational policies may result in loss of access privileges as well as appropriate disciplinary or corrective action in accordance with procedures outlined in the governing contractual agreement, if any. (See Faculty Status Agreement, Student Standards of Conduct, RHSHP Faculty Handbook, SPS Faculty Handbook, Human Resources Policy Manual, RHSHP Student Handbooks, Regis University Bulletin.) If such activity also violates local/state/federal laws, perpetrators may be referred to appropriate law enforcement officials.