

Kenrick-Glennon Seminary Computer Use Policy

In the words of Pope John Paul II in his January 24, 2005, apostolic letter entitled “The Rapid Development” directed to those responsible for communications, “Such is the importance of the mass media that fifteen years ago I considered it inopportune to leave their use completely up to the initiatives of individuals or small groups, and suggested that they be decisively inserted into pastoral programs.” The mandate to which this letter points is made clear in *Redemptoris Missio*, promulgated on December 7, 1990, which invokes the idea of the Areopagus, explaining that “[t]he means of social communication have become so important as to be for many the chief means of information and education, of guidance and inspiration in their behavior as individuals, families and within society at large. In particular, the younger generation is growing up in a world conditioned by the mass media.” This social conditioning brings about a deeper reality calling us to integrate the message of the Gospel into the ‘new culture’ modern communications has created. Based on this idea, “The Rapid Development” specifically addresses the rise of the Internet, which “not only provides resources for more information, but habituates persons to interactive communication” in addition to “other new means of communication” as tools that should become appropriate extensions of the Church’s mission in the world.

The importance of the Church’s becoming an active producer of cyberspace is outlined in two additional documents promulgated by the Pontifical Council of Social Communications on February 22, 2002, entitled “Church and Internet” and “Ethics in Internet.” The former document argues that “It is important, too, that people at all levels of the Church use the Internet creatively to meet their responsibilities and help fulfill the Church’s mission. Hanging back timidly from fear of technology or for some other reason is not acceptable, in view of the very many positive possibilities of the Internet.” That we in the seminary are responsible for ensuring this reality is made explicitly clear in the statement that “[p]riests, deacons, religious, and lay pastoral workers should have media education to increase their understanding of the impact of social communications on individuals and society and help them acquire a manner of communicating that speaks to the sensibilities and interests of people in a media culture. Today this clearly includes training regarding the Internet, including how to use it in their work.” The latter document argues that “the Catholic Church, along with other religious bodies, should have a visible, active presence on the Internet and be a partner in the public dialogue about its development.” The use of computing resources and the network at Kenrick-Glennon Seminary, therefore, is not only consistent with the mission and values of the institution and the Archdiocese of St. Louis and with local, state, and federal laws, but it is also consistent with the interests of the Vatican.

To ensure that Kenrick-Glennon Seminary engages this task responsibly, this policy Computer Usage Policy applies not only to the institution-owned computers and related equipment, but also to all computers and related equipment used on institution property but not owned by the institution as access to cyberspace from the institution occurs through an institutional network. Accountability is ensured through the institution’s

monitoring of all computing resources accessing the institution's network, and users are forbidden unauthorized access of cyberspace outside of the institutional resources established for that purpose and may not use for illicit purposes alternative means of accessing cyberspace (such as cell phones, dial-up, or local non-institutional wireless signals) to intentionally bypass network restrictions or institutional monitoring programs. Because computing resources on the institution grounds may not be used for illegal purposes, users are required to comply with all federal, state, and other applicable laws. This includes the laws of privacy, copyright, trademark, obscenity, and child pornography. The Electronic Communications Privacy Act and the Computer Fraud and Abuse Act prohibit "hacking," "cracking," and infringement of applicable software licenses.

Those uncertain of whether an activity violates a policy or law should seek guidance prior to engaging in the activity.

Examples of violations of the computer usage policy include, but are not limited to, the following as concerns institutional computers or personal computers that access the institutional network:

- Intentionally publishing, displaying, transmitting, retrieving, or storing inappropriate or offensive material.
- Creating or distributing defamatory, false, inaccurate, abusive, threatening, offensive, invidiously biased, discriminatory, or illegal material.
- Viewing or distributing obscene, pornographic, profane, or sexually oriented material.
- Gambling or illicit purchasing, including term papers and contraband drugs.
- Libeling, slandering, harassing, intimidating, or threatening others either within or outside the institution.
- Loading or attempting to load unlicensed software on institutional or personal computers.
- Willfully destroying or damaging equipment, software, or data belonging to the institution or other users.

Additionally, it is unethical to misuse the computing resources, interfere with the use of computing resources by others, or intimidate others. Examples include, but are not limited to, the following:

- Any unauthorized use of computing resources. Users are responsible for obtaining authorizations necessary for the use and operation of computing resources before using them. This includes off-task activity during classtime.
- Any unauthorized use of accounts or passwords other than those assigned to the user.
- Any unauthorized use of computing resources for commercial or personal

fundraising purposes including the unauthorized use of the educational status of the institution to promote such purposes.

- Any use or distribution of a program intended to damage or to place excessive load on a computing resource or the network. This includes, but is not limited to, programs known as computer viruses, Trojan horses, and worms.
- Any unauthorized monitoring of or tampering with another user's electronic communications, including any unauthorized reading, copying, changing, or deleting of another user's files or software.
- Any posting of materials on Blackboard, electronic bulletin boards, or other outside forums that violate existing federal, state, or local laws or violate the codes of conduct for this institution.

The Computer Usage Policy applies to the use of all Kenrick-Glennon computing resources. Additional computing resource and network-use policies, terms, and conditions may be in place or may be instituted in the future for specific electronic services offered by the institution.

Users are provided access to the Kenrick-Glennon institutional network with the understanding that they will adhere to the aforementioned policies. The institution extends to students, faculty, and staff the privilege to use its computing resources and network. This is not a right, and use of the computing resources may be revoked for violating any terms of this policy.

Users will be held accountable for their conduct under any applicable institutional policies, procedures, or codes of ethics and conduct. Complaints alleging misuse of institutional computing and network resources should be directed to the Office of Instructional Technology or those responsible for taking appropriate disciplinary action.

The Office of Instructional Technology typically handles minor infractions of this policy or those that appear accidental in nature. More serious infractions are handled via formal procedures. In some situations, it may be necessary to suspend account privileges to prevent ongoing misuse while the situation is under investigation.

Infractions by students may result in the temporary or permanent restriction of access privileges and referral of this situation to the Academic Dean and/or the Dean of Students. Infractions by a faculty or staff member may result in referral to the appropriate administrative officer.

Offenses that are in violation of local, state, or federal laws will result not only in the revocation of computing privileges as part of an institutional disciplinary action, but they will also be reported to the appropriate law-enforcement authorities.

No person under 18 years of age may use computing resources on the institution grounds unless that person has permission from an appropriate administrative authority and has appropriate supervision. There are no computing resources located on the institution grounds appropriately configured for Web surfing by minors.

Violations of this policy will result in disciplinary or legal action by the institution.

Some items within this policy were adapted from the policies in force at the following institutions:

- Georgia Southern University:
<http://academics.georgiasouthern.edu/provost/policies/computeruse.html>
- Ohio State University: http://cio.osu.edu/policies/responsible_use.html
- U.C. Berkley: <http://technology.berkeley.edu/policy/itpolicy/usepolicy.html>
- University of Georgia: <http://www.uga.edu/compsec/use.html>

KENRICK COMPUTER NETWORK

Windows XP Professional is preferred to Windows XP Home for full network access.

The institution will provide Norton antiviral software; the student need not install separate antiviral software on his system as it will conflict with Norton. (From Tony 9/8/2004)