

Marymount University's Computer Policy

Introduction

All users have the responsibility to use the Marymount University computing services in an efficient, ethical and legal manner, consistent with the goals of the University. Computer users are expected to abide by the following policies which are intended to preserve the utility and flexibility of the computer system, protect the work of students, faculty and staff, and preserve the right to access networks to which the University is connected.

These policies operate in conjunction with the University's Code of Academic and Community Conduct. These policies are representative but not all inclusive. Individual Marymount University computer laboratories may post additional operational rules and restrictions that are considered part of the Marymount University computer policy. Users are responsible for reading and following these rules.

Access

Users will be assigned a Marymount University computer account to access Marymount University computer facilities. The University reserves the right to access accounts and the system at any time at its sole discretion.

Your own password will allow access to your account. It is your responsibility to protect your account from unauthorized use by changing passwords periodically and by using passwords that are not easily guessed.

Identify yourself clearly and accurately in electronic communications. Concealing or misrepresenting your name or affiliation is a serious abuse. Using identities of other individuals as your own constitutes fraud.

Security

Accept responsibility for your own work by learning appropriate uses of software to maintain the integrity of what you create. Keep archives and backup copies of important work; learn and properly use the features for securing or sharing access to your files on any computers you use.

Any attempt to circumvent system security, guess other passwords, or in any way gain unauthorized access to local or network resources is forbidden. Distributing passwords or otherwise attempting to evade, disable or "crack" passwords or other security provisions threatens the work of many others and is therefore grounds for immediate suspension of your privileges. You may not develop programs or use any mechanisms to alter or avoid accounting for the use of computing services or to employ means by which the facilities and systems are used anonymously or by means of an alias.

The University cannot and does not guarantee the security of electronic files on its computer system.

Restrictions

Information Technology Services may impose limitations or restrictions on computing resources, such as storage space, time limits or amount of resources consumed when necessary.

Computer use for course related assignments takes priority over exploratory use. Information Technology Services may restrict access to certain programs for security or administrative purposes.

Users are expected to refrain from engaging in deliberate wasteful practices such as sending chain letters through electronic mail, printing unnecessary listings, printing multiple copies of files, performing unnecessary computations, or unnecessarily holding public terminals or dial-up phone lines for long periods of time when others are waiting for these resources.

Unauthorized transferring of copyrighted materials to or from the Marymount University computer system without express consent of the owner is a violation of federal law. In addition, use of the Internet from an educational site for commercial gain or profit is prohibited.

Use of electronic mail and other network communication facilities to harass, offend or annoy other users is forbidden. Obscene, defamatory or any other material which violates University policy on non-discrimination or the code of conduct will not be tolerated on the Marymount University computer system.

Facilities

You are expected to take proper care of the equipment in Marymount facilities. Food, drink and smoking are not permitted in University labs. Report any malfunctions to the lab assistant on duty or send e-mail to **'its@MARYMOUNT.EDU'**. Do not attempt to move, repair, reconfigure, modify or attach external devices to the systems.

Enforcement

Violations of policy may be treated as violations of University policy and/or as violations of civil or criminal law. Information Technology Services will investigate apparent or alleged violations of these guidelines. The Executive Director for Information Technology Services reserves the right to immediately suspend user privileges pending investigation. Such action will be taken to protect the security and integrity of the computer system and will take precedence over its impact on the individual's work.

When appropriate, at the discretion of the Executive Director, cases of apparent abuse will be reported to the Vice President for Student Services (student cases), the Vice President for Academic Affairs (faculty case), or the Vice President for Financial Affairs (staff cases). These offices are responsible for determining any further disciplinary action. Upon a finding of a violation, disciplinary measures may include warnings, suspension of user privileges (temporary or permanent), disciplinary probation, suspension or dismissal from the University. The University may also pursue civil and/or criminal charges if it deems appropriate.