

# Messiah College Computing Access Policy

## I. Purpose

This policy applies to anyone who uses the college's computers and networks and articulates the standards of behavior that are expected of all users. The college retains its legal ownership and right to use information residing or transmitted on college owned systems. With this policy, the college does not restrict in any way its legal right to monitor and control computing activity occurring on college owned systems and networks. The Chief Information Officer (CIO) is responsible to carry out this policy, and to make referrals to appropriate administrative offices when necessary. Any exception to this policy must be approved by the CIO. This policy is referenced in the Messiah College IT Security Plan.

## II. Policy

### A. Social Responsibility

Messiah College calls on everyone who is part of the college community to recognize the need for social responsibility. This includes but is not limited to the following implications:

1. Being good stewards of the environment. Examples include but are not limited to:
  - a. Using but not abusing the equipment provided, i.e. helping to make equipment last as long as possible.
  - b. Being conservative in the use of supplies.
2. Being respectful of others:
  - a. Ensure appropriate care is taken when using college owned or leased equipment and internal college information.
  - b. There are rules for the use of each specific computer lab, giving usage priority to different individuals based on Information Technology Services (ITS) discretion.
3. Confronting one another in love when necessary. We should try to resolve problems by talking with each other, and as situations dictate, report problems to governing college personnel. Examples include:
  - a. Accessing material on the internet that is inappropriate.
  - b. Ignoring usage guidelines for a particular lab.
  - c. Behaving in ways that could damage and/or disrupt access to college computing resources.

### B. Requirements

Users must abide by all applicable laws and government regulations, comply with policies on the appropriate use of various college computing facilities, and operate within the limits articulated by the college for ethical and moral behavior. Examples include but are not limited to:

1. Having appropriate status (staff, faculty, current students, alumni, etc.) and being properly authorized.
2. Being familiar with, and adhering to, guidelines such as are found in the computer lab manual.
3. Being in compliance with licensing agreements and copyright law related to software and other digital material.
4. Using software or data in a manner that does not infringe on the rights of others. Specific examples include avoiding the production or propagation of material that is abusive, profane, or sexually, racially or religiously offensive; or material that may injure or harass someone else, or lead to civil or criminal liability as determined by a court of law.
5. Using equipment connected to the college infrastructure to access off-campus resources (including materials on the internet) in a manner that is in compliance with the ethical and moral standards of the college. This includes the use of computers owned by the college and also personally owned computers connected to the college network. Examples include but are not limited to (a) being careful to avoid inappropriate material on the World Wide Web, and (b) respecting the copyrights on digital material such as MP3 files.
6. Minimizing personal use of college computing facilities such that usage is not excessive or contrary to the college's nonprofit purposes or stated standards.

### **C. Restrictions**

Users must not engage in activity outside the limits of access that have been authorized for them. This includes but is not limited to:

1. Performing an act that negatively impacts the operation of computers, peripherals or networks, or that impedes the ability of someone else to do his/her work. Examples include but are not limited to:
  - a. Tampering with any transmission medium or hardware device, or connecting any unauthorized device or computer to the college network.
  - b. Propagating a software virus or worm.
  - c. Damaging or destroying data owned by the college or someone else.
  - d. Modifying any disk or software directory provided by the college for any type of special use.
  - e. Performing an act that places an unnecessary load on a shared computer or the college network. Specific examples would be to play a network based computer game that significantly degrades the performance of the college network, or to download excessive amounts of data from the internet, or to set up a server that downloads excessive amounts of data to individuals who are off-campus.
2. Attempting to circumvent protection schemes for access to data or systems, or otherwise uncover security loopholes.
3. Gaining or granting unauthorized access to computers, devices, software or data. This includes, but is not limited to:

- a. Admitting someone into a locked facility, such as a computer lab, or unlocking any facility that is normally locked, without permission.
  - b. Revealing a password to any account, including one's own personal account, without permission.
  - c. Permitting the use of any account, including one's own personal account, in a way that allows unauthorized access to resources.
4. Monitoring someone else's data communications, or otherwise reading, copying, changing or deleting files or software without proper permission of the owner.
  5. Using the college's facilities to broadcast unauthorized personal messages to large segments of the college community. Examples include but are not limited to:
    - a. Advertising campaigns for personal financial gain or political purposes.
    - b. Pranks and chain messages.
    - c. Announcements not approved for dissemination by this method.
  6. Performing an act that breaks any applicable law or government regulation, including but not limited to the following:
    - a. Protecting Our Children Act
    - b. FTC Red Flags Rules (identity theft rules)
    - c. Gramm-Leach-Bliley Act
    - d. FERPA

#### **D. College Policies**

Users of the college computing environment must abide by all other applicable Messiah College policies. Examples include but are not limited to:

1. Messiah College Software Piracy Policy.
2. Authorization requirements and procedures; i.e. password and log-in requirements.
3. Usage restrictions, physical access regulations, and behavioral expectations established for each location containing equipment designated for public use. Examples: games policy, location specific software usage priorities (such as for some general labs and all special function labs), etc.
4. Usage requirements and restrictions for network connections in residence hall rooms.

#### **E. Enforcement**

At its own discretion, the college will enforce this policy. This includes, but is not limited to, the following implications:

1. Violations of this policy will be referred to appropriate administrative offices for disciplinary action. Violators will be subject to disciplinary outcomes as outlined in the Student Handbook and Employee Handbook. In addition to the other sanctions outlined in the handbooks, one possible outcome is the restriction or suspension of access privileges.

2. Material (software, hardware or data) that is found to be in violation of this policy may be banned, confiscated, or otherwise eliminated from the college computing environment.