Pine Manor College
Acceptable Use Policy

1.0 Introduction

As part of its educational mission, Pine Manor College acquires, develops, and maintains computers, computer systems and networks. These computing resources are intended for use by authorized members of the college community for college-related purposes, including direct and indirect support of the college’s instruction and service missions; college administrative functions; student and campus life activities; and the free exchange of ideas within and among the college community and the wider local, national, and world communities.

Pine Manor College values openness and promotes access to a wide range of information. Campus information systems have been designed to be as open as possible, and as such the College insists on responsible use of these systems. Because the electronic environment is easily disrupted and electronic information is readily reproduced, respect for the work and rights of others is especially important.

The College’s information systems consist of all networking, computing, and telecommunications wiring, equipment, networks, security devices, passwords, servers, computer systems, computers, computer laboratory equipment, workstations, Internet connections, cable television plant, and all other intermediary equipment, services and facilities currently in place or installed in the future. These assets are the property of Pine Manor College. This Appropriate Use Policy describes how these assets are permitted to be used.

To protect the integrity of computing and information resources against unauthorized or improper use, and to protect authorized users from the effects of unauthorized or improper usage, the College reserves the right, with or without notice, to monitor, record, limit or restrict any account holder’s access and/or usage. The College may also monitor record, inspect, copy, remove or otherwise alter any data, file, or system resources. The College reserves the right to periodically check these systems and to take any other actions necessary to protect the computer, network and telecommunications facilities or the information they hold, process, or transmit. The College also retains access rights to all files and electronic mail on its computing and network facilities. Anyone using these systems or networks expressly consents to such monitoring.

This policy applies to all users of college computing resources, whether affiliated with the college or not, and to all uses of those resources, whether on campus or from remote locations. Users of the College’s facilities are expected to adhere to this policy and, by accessing the system, the user agrees to comply with and be subject to this policy. These policy statements are intended to augment, not supersede, any additional contractual agreements of conduct or confidentiality to which a user may be subject. The College reserves the right to amend this policy at any time with or without notice.
Questions or comments regarding this document should be addressed to the Director of Information Technology Services, the Office of the President, or the Board of Trustees.

2.0 Rights and Responsibilities

The rights of academic freedom and freedom of expression apply to the use of college computing resources. So too, however, do the responsibilities and limitations associated with those rights. Pine Manor College supports a campus and computing environment open to the free expression of ideas, including unpopular points of view; however, the use of college computing resources, like the use of other college-provided resources and activities, is subject to the requirements of legal and ethical behavior. Thus, legitimate use of a computer, computer system or network does not extend to whatever may be technically possible.

Access to college computing and networking resources is a privilege available to all members of the Pine Manor College academic community. Certain responsibilities accompany that privilege. Understanding them is important for all technology resource users. The framework of responsible, considerate, and ethical behavior expected by the College extends to coverage of the use of all campus computers, campus network resources, and networks throughout the world to which the College provides computer access.

3.0 General Rules

3.1 Pine Manor College information systems may be used for lawful purposes only. Users must not use their accounts or College information systems for unlawful purposes, including, but not limited to, the installation of fraudulently or illegally obtained software, illegal dissemination of licensed software, sharing of content where the disseminator does not hold lawful intellectual property rights, propagating unlawful or deceptive schemes, or for any purpose contrary to local, state, and federal law or College policy.

Examples of applicable laws, rules and policies include, but are not limited to, the laws of libel, privacy, copyright, trademark, obscenity and child pornography, the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking," "cracking" and similar activities, the college's Student Code of Conduct, and the college's Harassment Policy. Users who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those jurisdictions and the rules and policies of those other systems and networks.

3.2 Users are responsible for ascertaining what authorizations are necessary and for obtaining them before using college computing resources. Users are responsible for any activity originating from accounts they can reasonably be expected to control. Accounts and passwords may not, under any circumstances, be used by persons other than those to whom they have been assigned by the account administrator. In cases when unauthorized use of accounts or resources is detected or suspected, the account owner or party that discovers the unauthorized use should immediately change the password and report the incident to the ITS Department.

3.3 Use of College information systems must comply with the provisions of the College’s Copyrighted Works Use Policy, copyright law and fair use. Copyright law limits the right of a user to decrypt, copy,
edit, transmit or retransmit another’s intellectual property without permission, including written materials, images, sounds, music, and performances, even in educational context, except where such use is in compliance with Fair Use or TEACH Act provisions.

3.4 The user is responsible for the correct use of the tools each computer system provides for maintaining the security of stored information. A summary of the relevant security is given below:

   a) Computer accounts, passwords, access cards, and other types of authorization are assigned to individual users and should not be shared with others. The person to whom an authorization is assigned will be held accountable for any activity originating from that account;

   b) The user should select an obscure password and change it frequently;

   c) It is incumbent upon every user to adhere to security policies and procedures and to call to the attention of the ITS Department and/or their supervisor those whom they feel are violating these procedures. Every effort will be made to ensure total anonymity, but it cannot be guaranteed;

   d) The computer user should be aware of computer viruses and other destructive computer programs, and take steps to avoid being either their victim or propagator.

3.5 Although there is currently no set bandwidth, CPU time, or other limit applicable to all uses of college computing resources, the college may require users of those resources to limit or refrain from specific uses if, in the opinion of the system administrator, such use interferes with the efficient operations of the system. These restrictions and limitations may be implemented at any time, with or without notice.

3.6 Users may not state or imply that they speak on behalf of the college or use college trademarks and logos without authorization to do so.

3.7 Users must not use computing resources to gain unauthorized access to remote computers on any network or to impair or damage the operations of Pine Manor College computers or networks, terminals or peripherals. This includes blocking communication lines, intercepting or monitoring communications, and running, installing or sharing virus or other malicious programs. Deliberate attempts to circumvent data protection or other security measures are not allowed.

3.8 Electronic messages pertaining to the official business of the College, including all academic and administrative matters, shall be sent from College-owned or other College-recognized messaging systems. For example, student inquiries must be sent from Pine Manor or other college-recognized email accounts. Replies from faculty or staff must be sent to the same accounts. In cases where unrecognized third-party messaging systems are used to originate a message, and/or where a party chooses to forward messages from a College-owned or College-recognized system to a third party unrecognized system, individuals using these systems shall be solely responsible for all consequences arising from such use.

3.9 Pine Manor College reserves the right to reject from the network or block electronic communications and content deemed not in compliance with policies governing the use of information systems, including with respect to an investigation of alleged misconduct or wrongdoing and/or to law
enforcement, pursuant to lawful inquiries and/or legal process. By accessing Pine Manor College information systems, users give the College permission to conduct each of the options described above.

3.10 The College reserves the right at any time, without prior notice or permission from the user or users of a computer or other College-owned computing device, to seize such devices and/or copy or have copied, any and all information from the data storage mechanisms of such devices as may be required in the sole discretion of the College in conjunction with investigations of possible wrongdoing.

3.11 Theft, vandalism, destruction, modification, or intentional damage to any Pine Manor College computer, network, equipment or data is prohibited.

3.12 By accessing and/or using any Pine Manor College information or telecommunications system, including its network, email, or Internet services, the user agrees and expressly consents to the terms of this policy, and gives Pine Manor permission to conduct each of the operations, monitoring, or oversight practices described in this policy.

4.0 Security & Privacy

4.1 The college employs various measures to protect the security of its computing resources and user accounts. Users should be aware, however, that the college cannot guarantee security and confidentiality. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords and changing them regularly.

4.2 Users should also be aware that their uses of college computing resources are not completely private. While the college does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the college's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns and other such activities that are necessary for the provision of service. The college may also specifically monitor the activity and accounts of individual users of college computing resources, including individual login sessions and the content of individual communications, without notice, when:
   a) The user has voluntarily made them accessible to the public, as by posting to Usenet, Web page, social networking site, blog, or any other publicly accessible system or forum;
   b) It reasonably appears necessary to do so to protect the confidentiality, integrity, or availability of college or other computing resources or to protect the college from liability;
   c) There is reasonable cause to believe that the user has violated or is violating this or any other applicable policy or local, state, or federal law;
   d) An account appears to be engaged in unusual or unusually excessive activity, or;
   e) It is otherwise required or permitted by law.

4.3 The College’s information systems, and the messages, email, files, attachments, graphics, and network traffic generated through or within these systems are the property of the College. They are not the private property of any College employee, faculty, staff, contractor, student, or any other person. No user of College systems should have an expectation of privacy in their electronic communications. All electronic communications, files, and content presented to or passed on Pine Manor networks, including those to, from, or through Internet connections, may be monitored, examined, saved, read,
transcribed, stored or re-transmitted by an authorized employee or agent of the College, in its sole discretion with or without prior notice to the user. The College reserves and intends to exercise the right to do so. Electronic communications and content may also be examined by automated means.

4.4 The electronic privacy rights of other users shall be respected at all times. Use of audio, video, cell phone, “web cam” or related technologies, for the purpose of capturing images and/or recording speech in locations or circumstances where a reasonable expectation of privacy exists, is prohibited without the prior consent of the subject(s) depicted and/or recorded. These provisions shall not apply to lawful surveillance conducted by appropriately authorized law enforcement agencies or Campus Safety. The College reserves the right to impose additional restrictions on the use of electronic recording devices, at its sole discretion.

4.5 Any such monitoring of communications, other than what is made accessible by the user, required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the appropriate administrative department. The college, at its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate college personnel or law enforcement agencies and may use those results in appropriate college disciplinary proceedings.

4.6 Requests for the disclosure of confidential information will be governed by the provisions of the various local, state, and federal laws that apply, including, but not limited to:
   1. Family Educational Rights and Privacy Act of 1974 (FERPA)
   2. Healthcare Insurance Portability and Accountability Act (HIPAA)
   3. Massachusetts Data Protection Regulation (201 CMR 17.00 and 93H)
   4. Payment Card Industry Data Security Standard (PCI-DSS)
   5. FTC Red Flags rules

All such requests will be honored only when approved by College officials who are the legal custodians of the information requested, or when required by state or federal law, or court order. Users found to be copying, modifying, or otherwise accessing information for which they have not been granted permission, or using information in an unauthorized manner, will be subject to disciplinary action, up to and including termination and prosecution.

5.0 Inappropriate Usage

Users must be sensitive to the public nature of shared facilities. Behavior reflects both upon the individual and the College. Computing and networking resources should be used only in accordance with this policy. Any intentional behavior with respect to the electronic environment that interferes with the missions or activities of the College or members of the College community will be regarded as unethical and may lead to disciplinary action under standard College rules for misconduct and existing judicial, disciplinary, personnel, or legal processes.

Examples of inappropriate and unacceptable use of computing and networking resources include, but are not limited to, the following:
1. Destruction of, unauthorized removal of, or damage to equipment, software, or data belonging to Pine Manor College or other users;
2. Disruption or unauthorized monitoring of electronic communications;
3. Tampering, modification, or additions to network software, hardware, or wiring. This includes installing, removing, or modifying software or hardware that has not been explicitly approved by the ITS Department;
4. Generation of excessive network traffic exceeding levels which create errors or performance problems for other users. Applications or computer hardware found to cause such problems may be moved to a different location or removed from the network, at the discretion of the network management staff;
5. Willful violations of computer system security;
6. Use of e-mail or messaging services to harass, intimidate, or otherwise annoy another person, for example, by broadcasting unsolicited messages or sending unwanted mail. Some mass mailings may be authorized by the appropriate College authority. This also applies to material originating from this campus but sent to other sites or persons on the Internet;
7. Use of College information systems to harass, threaten, defame or intimidate any individual or group;
8. Generate and/or spread intolerant or hateful material, which in the sole judgment of the College is directed against any individual or group, based on race, religion, national origin, ethnicity, age, gender, gender identification, marital status, sexual orientation, veteran status, genetic makeup, or disability;
9. Transmit or make accessible material, which in the sole judgment of the College is offensive, violent, pornographic, annoying or harassing, including use of College information systems to access and/or distribute obscene or sexually explicit material unrelated to College sanctioned work or bona fide scholarship;
10. Generate unsolicited email such as chain letters, unsolicited job applications or commercial announcements;
11. Generate falsely identified messages or message content, including using forged content of any description;
12. Transmit or make accessible password information;
13. Attempt to access and/or access information systems and/or resources for which authority has not been explicitly granted by the system owner(s);
14. Capture, decipher or record user IDs, passwords, screenshots, or keystrokes;
15. Manipulate or tamper with uniform resource locators (URLs);
16. Intercept electronic communications not intended for the recipient;
17. Probe by any means the security mechanisms of any resource on any College network, or on any other network through a connection to the College network;
18. Disclose or publish by any means the means to defeat or disable the security mechanisms of any component of a College information system or network;
19. Alter, degrade, damage, or destroy data;
20. Transmit computer viruses or malicious/destructive code of any description;
21. Conduct illegal, deceptive, or fraudulent activity;
22. Obtain, use or retransmit copyrighted information without the permission of the copyright holder;
23. Place bets, wagers, or operate games of chance;
24. Tax, overload, impede, interfere with, damage or degrade the normal functionality, performance or integrity of any device, service or function of College information systems, content, components, or the resources of any other electronic system, network, service or property of another party, corporation, institution or organization;
25. Use of computer accounts, access codes, or network identification names or numbers other than those assigned to you;
26. Use of computer and/or network facilities in ways that impede the computing activities of others (for example, randomly initiating interactive electronic communications or e-mail exchanges, overuse of interactive network utilities or applications, playing games on shared resources, or the overuse of network-accessible discussion lists or file-transfer sites);
27. Setting up network servers or network services (such as naming and/or address servers, Web servers, dial-in access, file servers, peer-to-peer applications, etc.) without the prior written authorization of the network management staff. Unauthorized activity of this type may be detrimental to the overall operation of the network and is not allowed;
28. Users must not attempt to implement their own network infrastructure. This includes, but is not limited to basic network devices such as hubs, switches, routers, network firewalls, and wireless access points. Users must not offer alternate methods of access to PMC IT resources such as modems and virtual private networks (VPNs). Users must not offer network infrastructure services such as DHCP and DNS;
29. Intentionally creating, displaying, printing or transmitting information which violates the college's harassment policy, including images, text, and media files;
30. Use of computing facilities for financial gain or commercial purposes unrelated to the mission of the College;
31. Use of computing facilities to solicit money, consideration, or participation in non-College sanctioned events or causes;
32. Violation of software copyrights and usage licensing agreements;
33. Violation of the usage policies and regulations of the networks of which Pine Manor College is a member or has authority to use;
34. Academic dishonesty (for example, plagiarism or cheating).

The above enumeration is not all-inclusive. If there is a question as to whether a specific use is appropriate or acceptable under this policy, the College’s sole determination will prevail.

6.0 Enforcement

Any unauthorized, inappropriate, illegal or illegitimate use of the College’s computing and information resources or failure to comply with these guidelines shall constitute a violation of College policy and subject the violator to disciplinary action by the College, up to and including termination of employment or relationship, and may result in legal action.

Alleged violations will be handled through the college disciplinary procedures applicable to the user. The college may suspend, block or restrict access to an account, independent of such procedures, when it reasonably appears necessary to do so in order to protect the confidentiality, integrity, or availability of college or other computing resources or to protect the college from liability. The college may also refer suspected violations of applicable law to the appropriate law enforcement agencies.
7.0 Sanction and Appeal Process

Violation of the policies described herein for use of computing resources will be dealt with seriously. Violators are subject to the disciplinary procedures of the College. Violators may lose computing privileges or account and network access, and may also be subject to prosecution by state and federal authorities under laws including, but not limited to, The Privacy and Protection Act of 1974, The 1986 Electronic Communications Privacy Act, and The Computer Fraud and Abuse Act of 1989. The sanction and appeal process may vary, depending upon the classification of the offender (student, faculty, or staff) within the College community.
I have read and agree to abide by the Pine Manor College Acceptable Use Policy.

Name

Date