Student Acceptable Use of College Computing Resources Procedure

Moraine Park Technical College provides access to computer systems and networks it owns or operates to Moraine Park Technical College students in order to promote legitimate educational and administrative efforts in keeping with the College's role as an educational institution. Such access has broad impact and imposes certain responsibilities and obligations. Students have the responsibility to use these resources in an efficient, ethical and responsible manner, consistent with the law, college policy and the mission of the College.

College Information Technology Systems and Resources (hereafter referred to as IT Systems)

The College provides computers, hosted systems, data networks, printers, telephone system, video conferencing, Internet access, online storage media, software, and data files including voice and video formats that are owned, managed, or maintained by Moraine Park Technical College. IT Systems also include institutional and departmental information systems and the College's wired and wireless campus networks, third party social networking web sites such as Facebook, Twitter, Blogger, LinkedIn, YouTube, etc. and any other web site that is used for College business.

Appropriate Student Use of IT Systems

IT Systems may be used only for their authorized purposes which are to support the educational, clinical, administrative, and other functions of Moraine Park Technical College. IT Systems provided by the College are for the exclusive use of students only and not friends, family members, etc. IT Systems are not for personal use and they are not to be used as a medium for free expression when unrelated to the academic programs or administration of the college.

A. **Unauthorized Use**. The following categories of use are inappropriate and prohibited:

1. **Use that Impedes, Interferes with, Impairs, or Otherwise Causes Harm to the Activities of Others**. Students must not deny or interfere with or attempt to deny or interfere with service to other users in any way, including by "resource hogging," misusing mailing lists, propagating "chain letters" or virus hoaxes, "spamming" (spreading Email or postings widely and without good purpose), or "bombing" (flooding an individual, group, or system with numerous or large Email messages). The distribution of unwanted and unauthorized Email, chain letters, or other unwanted messages is prohibited. Other behavior that may cause excessive network traffic or computing load such as peer-to-peer networking is also prohibited.

2. **Use that is Inconsistent with Moraine Park Technical College's Non-Profit Status**. The College is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state, and local laws regarding sources of income, political activities, use of property, and similar matters. As a result, Moraine Park Technical College IT Systems are not to be used for commercial activities that do not relate to the direct business of the college. Such activities include connections to and business on or over the Internet either involving creation of Internet commerce sites or the sale or re-sale of goods and services through sites available through connection to other computers on the Internet or private business locations, except if specifically authorized and permitted under College conflict-of-interest, outside employment, and other related policies. Prohibited commercial use does not include communications and exchange of data that furthers the College's educational, administrative, clinical, and other roles, regardless of whether it has an incidental financial or other benefit to an external organization.

3. **Political Use.** Use of IT Systems in a way that suggests College endorsement, support, or opposition of any political candidate or ballot initiative is also prohibited. Users must refrain from using IT Systems for the purpose of lobbying that connotes College involvement.

4. **Harassing or Threatening Use**. This includes, but is not limited to, using IT Systems to disparage or threaten others or in a manner considered to be harassing, discriminatory, menacing, obscene, defamatory, or in any way objectionable or offensive based on their race, religion, color, sex, sexual orientation, national origin, veteran status, disability, ancestry, or age.

   Using the Internet, Email, telephone, Instant Messaging, video conferencing, fax, or other technologies to send, receive, solicit, print, copy, or reply to any text or images for the following purposes is strictly prohibited:

   a. Spreading gossip rumors and innuendos about others; using foul, obscene, off-color, or adult-oriented language; sending sexually oriented messages or images; creating alarm, embarrassing the College, or negatively impacting or harming students;

   b. Harassment or annoyance of others, whether through language, frequency or size of messages, or number and frequency of telephone calls; and

   c. Communicating with any person who does not wish to receive it, or with whom you have no legitimate reason to communicate.

5. **Use Damaging the Integrity of College or other IT Systems**. This category includes, but is not limited to, the following activities:

   a. **Attempts to Defeat System Security**. Students must not defeat or attempt to defeat any IT Systems' security. Examples are "cracking" or guessing and applying the identification or password of another User, compromising room locks or alarm systems, breach, test, monitor computer or other electronic media security measures, defeat anti-virus, anti-spam or other filters, or interfere with the operating system or software application patching process. This provision does not prohibit IT from using security scan programs within the scope of their responsibility.

   b. **Unauthorized Access or Use**. The College recognizes the importance of preserving the privacy of Students and data stored in IT Systems. Students must honor this principle by neither seeking to obtain unauthorized access to IT Systems, nor permitting or assisting any others in doing the same. For example, no outside Moraine Park Technical College organization or individual may use IT Systems without specific authorization. In addition, no privately owned computer or network may be used to host sites or services for Moraine Park Technical College organizations or individuals without specific authorization. Students are prohibited from accessing or attempting to access data on IT Systems that they are not authorized to access. Students must not make or attempt to make any deliberate, unauthorized changes to data on an IT System. Students must not intercept or attempt to intercept or access data communications not intended for that user, for example, by unauthorized network monitoring, running network sniffers, or otherwise tapping phone or network lines.

   c. **Disguised Use**. Students must not conceal their identity when using IT Systems, except when the option of anonymous access is explicitly authorized, including but not limited to Emails from the College and responding to College surveys. Students are also prohibited from masquerading as or impersonating others or otherwise using a false identity to send Email, etc.

   d. **Distributing Computer Viruses and Rogue Programs**. Students must not knowingly distribute or launch computer viruses, malware, worms, or other rogue programs to any IT Systems.

e. **Modification or Removal of Data or Equipment**. Without specific authorization, Students may not remove or modify any College-owned or administered equipment or data from IT Systems.

f. **Use of Unauthorized Devices.** Without specific authorization, Users must not physically connect any additional device, including but not limited to PCs, laptops, routers, network switches, wireless access points, network server, network sniffer, or external device for additional data storage or backup of data, printer, or video and voice systems to IT Systems.

g. **Use of Unauthorized Software.** Students may not download or install unauthorized software when using IT Systems.

6. **Use in Violation of Law.** Illegal use of IT Systems, that is, use in violation of civil or criminal law at the international, federal, state, or local levels is prohibited, including but not limited to promoting a pyramid scheme; distributing offensive material; receiving, transmitting, or possessing child pornography; infringing copyrights; and making bomb threats.

   With respect to copyright infringement, Students should be aware that copyright law governs (among other activities) the copying, display, and use of software and other works in digital form (text, sound, images, and other multimedia). The law permits use of copyrighted material without authorization from the copyright holder for some educational purposes (protecting certain classroom practices and "fair use," for example), but an educational purpose does not automatically mean that use is permitted without authorization. Questions regarding copyright infringement should be directed to the District Libraries Associate.

7. **Use in Violation of College Contracts**. All use of IT Systems must be consistent with the College's contractual obligations, including limitations defined in software and other licensing agreements.

8. **Use in Violation of District Board Policies and College Procedures**. Use in violation of policies and procedures also violates this Acceptable Use Procedure. Relevant policies and procedures include, but are not limited to, those regarding sexual harassment and racial and ethnic harassment.

9. **Use in Violation of External Data Network Policies**. Students must observe all applicable policies of external data networks such as eCollege and social networking sites when using such networks.

10. **Telephone System (VoIP) Use.** Phones must not be moved, disconnected, or otherwise altered. Phones are provided for business use and personal use should be limited to emergencies.

B. **Student Responsibilities**

1. **Equipment Care.** Students are responsible for maintaining the condition of their College issued equipment. This includes keeping technology clean from food, drinks, cigarette ashes, stickers, etc. Equipment taken off site should be secured and kept in a clean, temperature-controlled environment.

2. **Personal Account Responsibility**. A student must have a network user ID and password to use any College computer.

   a. Students are responsible for maintaining the security of their own IT Systems login ID and passwords as follows:
      i. Login IDs and passwords are assigned to single Students and are not to be shared with any other person or entity as the Student is responsible for any activity, authorized or not, that is carried out with their IT Systems login. When finished using a computer in a lab, you must

logoff the computer to protect your private information and to prevent another person from acting maliciously using your login information. When necessary, login ID and passwords must be shared with college IT staff after they have provided acceptable identification.

ii. Students must not disclose their login ID and/or password via a link in any Email received. The College will never request students to provide this information via Email. Students must be aware that phishing emails (phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication) will be received requesting them to disclose their login ID and password. Disclosing this information puts all college data at risk.

iii. Passwords are to be kept secure from others e.g., they should not be posted on monitors or notes kept on desk tops that allow others to access them.

b. Characteristics of passwords:

i. After 15 failed login attempts the account will be locked. The account will be automatically unlocked after 15 minutes. If the account must be unlocked sooner, the user may contact the Central Help Desk for assistance.

ii. User password changes must follow these guidelines:

1) Minimum password length is 8 characters
2) Must not contain your account name or parts of your full name that exceed two consecutive characters
3) Must contain characters from three of the following four categories:
   a) English upper-case characters (A through Z)
   b) English lower-case characters (a through z)
   c) Base 10 digits (0 through 9)
   d) All other keyboard characters except for $ @

iii. User passwords will automatically expire after 180 days from the date of last change. On the date of expiration a new password must be selected. The new password must be one that was not previously used.

3. **Student Data.**

All electronic data stored in computing equipment (Email, voice mail, data files, etc.) is the property of the College and it is the College's responsibility to review and ensure that students are operating within the laws as covered by state and federal statutes. The College is not liable for loss of data because of systems failures, emergencies or the unauthorized access, use, or corruption of data by any individuals.

One category of data that is especially sensitive is Personally Identifiable Information (PII) which is usually defined as any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

PII is defined as the first name or initial and last name "in combination" with one or more of the following nonpublic unencrypted pieces of information:

a. A social security number or national ID;
b. Employer identification number;
c. Student identification number;
d. Passport number;
e. Mother's maiden name;
f. Date of birth;
g. Driver's license number or other photo identification card number;
h. Bank account, credit card or debit card number accompanied by the applicable passwords or security codes;
i. Payroll and salary information;

j. Or medical information.

"In combination" is defined as the personal information being contained in the same document or database or contained within separate documents or databases on the same electronic hard drive or media such that the name and the other personal information can be associated together. e.g. a social security number which can be associated with the name of the owner.

It is the responsibility of each student to protect the information and data files to which they have access. PII should never be stored on College provided network storage.

Acceptable Data. Only data required to perform or support student course work should be stored on College provided storage. However, students may utilize the storage capabilities available via their Live@edu accounts to store data provided it meets the requirements of Microsoft's acceptable use policies and does not contain any PII data.

Software Management and Licensing. All computer software used by members of the Moraine Park Technical College community must be properly and legally licensed and used. Moraine Park Technical College licenses the use of many different software programs from vendors and developers. In addition, students may purchase software through Moraine Park Technical College with licensing and use agreements. All Moraine Park Technical College students are required to use software in accordance with the appropriate licensing agreements. Failure to do so can result in significant legal liability, for the student. The fact that Moraine Park Technical College is an educational institution does not confer rights to copy or use software in any way not authorized by the provisions of licensing and use agreements. The unauthorized duplication or use of any software that is licensed or protected by copyright may constitute violations of civil and criminal law, and is prohibited by this policy.

College Internet Filtering. The Information Technology Department utilizes software to prevent the viewing of content which the College considers objectionable.

USB Flash Drives. The Information Technology department recommends that students purchase their USB flash drives from the campus bookstore. Flash drives come in a variety of brands/models/features, and Information Technology wants to ensure student's flash drives are compatible with the rest of the technology in our computer labs. Flash drives are not supported by the Information Technology department.

Personal Identification. Upon request Students using IT Systems must produce valid identification.

College Rights of Access.

The College places a high value on privacy and recognizes its critical importance in an academic setting. There are nonetheless circumstances in which, following carefully prescribed processes, the College may determine that certain broad concerns outweigh the value of a Student's expectation of privacy and warrant College access to relevant IT Systems.

As owner or operator of College electronic communications systems, Moraine Park Technical College has proprietary rights of access, regulation of use and resource allocation and management. The College may exercise these rights when it deems it appropriate and in the best interests of the College. Therefore, the Information Technology Department has the authority to monitor all computing resources. Every effort will be made to maintain privacy and security in this process.