| Policy Name: | Policy on Acceptable Use, Information Technology | | |
|---|---|---|---|
| **Department** | Admission | **Approval Authority** | Rector |
| **Date of Implementation** | 21/07/2020 | **Date of last Revision** | 21/07/2020- V01 |

1. **Introduction of Policy**

   MI College's information technology (IT) resources are intended to support the educational, administrative, and campus life activities of the College. The use of these resources is a privilege extended to members of the MIC community, who are expected to act in a responsible, ethical, and legal manner. In general, acceptable use entails behavior that respects the rights of others, does not compromise the security or integrity of IT resources, and complies with all applicable laws and license agreements.

2. **Scope**

   This policy applies to all users of IT resources owned or managed by MI College. IT resources include all College owned, licensed, or managed hardware and software, as well as the College network, regardless of the ownership of the device connected to the network, the means of connecting, or the locale from which the connection is made.

3. **Protocols**

   a. **Acceptable Use of College Information Resources.** MI College Information Resources are provided for faculty, staff and students to be used in the pursuit of the teaching, educational and service mission of the college. Administrative activities that are part of the support infrastructure needed for instruction, scholarship, and institutional management of the member institutions.

   b. **Data Protection Copyright.** All confidential information transmitted over external networks or saved on system servers must be encrypted, must not be sent or forwarded through non-MI College email accounts (like Hotmail, Yahoo mail, AOL mail, etc.), and must not be knowingly transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols and security techniques are utilized. Users of Information systems must not attempt to access data or programs contained on systems for which they do not have authorization by the system owner.

   c. **Laws and regulations.** Users must comply with all applicable law; all applicable MI College rules and procedures; and all applicable licenses and

contracts. Examples include but are not limited to laws pertaining to libel, copyright, trademark, child pornography, and hacking; the College's code of student conduct; the College's Principles of Intellectual Honesty; the College's sexual harassment policy; and all applicable software licenses.

d. **Internet Use.** All computers and/or portable-computing devices using MI College Information Resources must be password protected and be changed when prompted according to the password authentication policy timeline of every 90 days or if the password is suspected of being compromised. Employees accessing the MI College network from a remote computer must adhere to all policies that apply to use from within MI College facilities, must conform to the IT minimum standards for portable computing, and are subject to the same rules and security related requirements that apply to college owned computers. All hardware that connects to the MI College network must be installed by a Certified Office of Technology technician and/or network administrators.

e. **Passwords.** Users may not attempt to evade, disable, or "crack" passwords or other security provisions. These activities threaten the work of others and are grounds for immediate disciplinary action. Unauthorized copying of files or passwords belonging to others or to the college will be considered as plagiarism or theft. Modifying files without authorization (including altering information, introducing viruses or Trojan horses, or damaging files) is unethical, may be illegal, and can lead to disciplinary action.

f. **Authorization.** Users may use only those IT resources they are authorized to use, in the manner and to the extent authorized, and they must not attempt to subvert or bypass college-imposed security mechanisms. Ability to access computers, computer accounts, computer files, or other IT resources does not, by itself, imply authorization to do so. Accounts and passwords may not be shared with or used by persons other than those to whom they have been assigned by the college. Users must make a reasonable effort to protect passwords and secure resources against unauthorized use.

g. **Fair Share of Resources.** Users must respect the finite capacity of the College's IT resources and limit their use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users. Information Technology Services may set limits on an individual's use of IT resources or require that an individual user refrain from specific uses in order to assure that these resources can be used by anyone who needs them. Reasonableness of use will be assessed in the context of all relevant circumstances, but any use that degrades the performance of the

College network or interferes with the ability of others to use IT resources or with the College's educational or business activities will be considered unacceptable.

h. **Personal Use.** Users may not use IT resources to campaign for or against a candidate for political office or for commercial purposes inconsistent with the College's tax-exempt status. Personal use of College IT resources for other purposes is permitted when it does not interfere with the performance of one's job or other College responsibilities, does not compromise the functionality or degrade the performance of IT resources, does not consume a significant amount of IT resources, and is otherwise in compliance with this policy. Further limits on personal use by College employees may be imposed in accordance with normal supervisory practices.

i. **Privacy and Security.** The College takes various measures to protect its information resources and users' accounts. However, you should be aware that the College cannot guarantee privacy and that it is the responsibility of individual users to engage in prudent practices by establishing appropriate access restrictions for their accounts and safeguarding their passwords.

   The normal operation of the College's IT infrastructure requires backing up data, logging activity, monitoring general usage patterns, and other such activities. While the College does not generally review the content of information contained on a computer or transmitted over the network, exceptions are made under the following conditio:

   i. when required to preserve public health and safety;
   ii. when required to preserve or restore system integrity or security;
   iii. when required by federal, state, or local law; or
   iv. when there are reasonable grounds to believe that IT resources are being used in violation of law or College policy.

j. **Enforcement.** Violations of this policy will be handled according to normal disciplinary procedures. However, a user's IT use privileges may be temporarily suspended by Information Technology Services prior to the initiation or completion of these procedures when there is a reasonable basis to believe that an individual is in violation of this policy.

k. **Oversight of E-resources.** Authorized employees of the College, including the IT staff delegated with the daily administration of the College's e-resources, may:

   i. Take all reasonable steps necessary to preserve the availability and integrity of E-resources, including blocking any user's access to e-resources.

ii. Exercise administrative authority over networks, systems, or software in order to grant users access to read, write, edit, or delete information in files or databases, to establish security controls and protection for information and e-resources, or to address claims that intellectual-property or other rights have been violated.
iii. Employ a variety of security monitoring devices and tools to identify misuse or unauthorized use of e-resources.
iv. With the approval of the Chief Executive Officer, temporarily shut off the College's Internet connection, servers, or services, without prior notice, in order to protect College systems, data, and users or to protect other important interests of the College.
v. Exercise administrative rights over certain e-resources, if those rights are delegated by the IT staff.

l. **Changes to this Policy.** The College reserves the right to change this policy at any time. The College will post the most up-to-date version of the policy on the College web site and may, in its discretion, provide users with additional notice of significant changes.

4. **Reference**

5. **Appendix**

**END OF DOCUMENT**