IT Policy & Procedure Handbook

1st reading by the Ad-hoc committee: 2/15/2022
2nd reading by ITC 2/22/2022
Approved by ITC 4/6/2022 (Email approved)
Approved by EC_07/22/2022

CMI POLICY NO. 640.01

Series 600: General Administrative Policies
Section 640: Other Policies

Acceptable Use Policy for Information Technology

Status:
Effective Date:
Steward:
Approval Authority:

1. Policy Statement

The college information technology provides students, faculty, staff, and community-wide access to information technology resources for its users' teaching, learning, research, organizational, and management activities. It safeguards data and information for the college. The goal of the Information Technology infrastructure at the college is to support it in achieving its mission, vision, and values. The technology resources may not be used to violate, interfere, disrupt, or exhibit action generally considered a breach of the existing college's policies and any national information technology laws and regulations or guidelines or court proceedings related to such, as well as offensive or improper usage of the community.

2. Reason for the Policy

This policy applies to the entire CMI community of students, employees (both faculty and staff), affiliates, and authorized guests. CMI requires all individuals to responsibly collect, process, store, and disseminate the information and technology. Endorsement of this policy shall be acknowledged before being allowed access to CMI information technology.

This policy complies with other CMI policies and procedures, particularly **HR policies & Student Handbook**, ensuring a harassment-free, discrimination-free, respectful, professional education/work environment.

3. Definitions

As defined by this policy, College information technology refers to information about people, objects, events, and derivations of these data. Information may be text, sounds, and images electronically and on paper and other tangible media. Information or data shall be subject to appropriate and consistent protection, whether in transit, stored in a shared server, cloud storage, workstation, laptop, personal digital device, file cabinet, copier, fax, database, or other possible locations. Information created using CMI information technology is an asset of the college. The information may include confidential and restricted information as well as public information.

Information technology (IT) is computer applications and telecommunications equipment to store, retrieve, transmit, and use data. CMI information technology includes all hardware, software, and communication networks that CMI owns, leases, or assigned control. It also contains non-CMI hardware and software connected to the college communication network or other college information technology. The information technology is owned, licensed, and subject to college policies.

Types of Users

Regular Users are approved to regularly use the College Information Technology resources. Only current students and full-time college employees are considered Regular users. Faculty, Students, and Staff status do not extend to family members or friends.

Special Users are those approved to use specific, limited Information Technology of the College for specific purposes under specific conditions. The special users consist primarily of individuals or organizations affiliated with the college. The special users also include working temporarily at the college under the direct sponsorship or contract of an administrative or academic department.

Guest Users- are defined as the temporary user for specific access such as the CMI public library or CMI wireless access. Only the Information Technology department can provide the guest users account for visitors and guests. The guest account is usually good for one day only, but it can be extended as per the approval of the requesting Department.

4. Statements of Elaboration of Policy

Statement of Responsibilities.

The college owns computers and all the technology equipment connected to networks. The college also has diverse rights to the software and information residing on, developed, or licensed for these computers and networks. The college (including central organizations, divisions, and departments) administers, protects, and monitors this aggregation of computers, software, and networks. In its management of information technology, the college and its administrative and academic departments take responsibility for focusing central information technology resources on activities connected with instruction, research, and administration:

5. Procedures

The college is responsible for the following:

- Assure that the college computer systems do not lose critical information because of hardware, software, or administrative failures or breakdowns.
- Provide students with the best possible hardware, software, sustainable maintenance services, and uptime.
- Protect college networks and other shared facilities from malicious or unauthorized use.
- Manage computing resources for fair access to members of the college community.
- Establish and support reasonable security standards for electronic information that community members produce, use, or distribute, and ensure the appropriate access levels, layered privacy, and accuracy of administrative data that the college maintains.
- Delineate the limits of privacy through transparent and approved processes and procedures that can be expected in using networked computer resources and preserving freedom of expression over this medium without countenancing abusive or unlawful activities.
- Monitor policies and communicate any changes in policy and procedure as events or technology warrant.
- Enforce policies by restricting access and initiating disciplinary proceedings as appropriate.

The college may designate to the Information Technology Department the responsibilities outlined above.

Student Computer Labs Rules and Regulations

The primary purpose of CMI student lab facilities is to complete academic coursework, such as class assignments requiring college-owned software and hardware. Non-academic services of college-owned hardware, software, and network bandwidth will be accommodated in the student lab facilities whenever possible. IT staff members (or official designees) have the right to limit the use of hardware and bandwidth for non-academic purposes.

Lab Hours and Maintenance

Labs are usually open during workdays to meet student needs. Changes or special lab hours are often posted in advance. Repairs or maintenance of labs shall cause minimal disruption to students' access or usage of labs. The IT Department communicates the scheduled lab maintenance or repair period to its users, which falls on less-disruptive hours.

1st reading by the Ad-hoc committee: 2/15/2022
2nd reading by ITC 2/22/2022
Approved by ITC 4/6/2022 (Email approved)
Approved by EC_07/22/2022

Kiosk Printing Stations
The college has provided free-of-charge self-service printing stations. But unfortunately, the outcome of this great practice creates waste - printed papers are often discarded, or documents are never collected and left in the computer labs. To address this, the IT Department provides a campus printer kiosk for students who need to print a document using their cloud printing account.
Payment: The printer kiosk accepts vouchers purchased from the bookstore.

The IT Department generally suggests appropriate printers and ink before purchase. College-owned printers are the responsibility of the IT Dept. The Department budget covers the costs of ink for computer labs.
The IT Department reserved the right to close a lab facility with little or no notice to users to address serious threats or emergency repair purposes. Regular maintenance hours may vary during vacation periods, summer sessions, and midterm recesses.

- Our Computer laboratories are open to all registered students currently taking classes at CMI.
- Always treat the computer laboratory equipment and your instructor and classmates the way you want your belongings and yourself to be treated.
- Food, drink, smoking, and betelnut are not allowed in computing facilities. Anyone found with food, or beverages will be asked to dispose of them or leave the facility.
- Some links can contain viruses or malware. Others may contain inappropriate content. Please ask your instructor if you are unsure if a website is safe.
  Non-registered students, such as minors or dependent adults, are not allowed in the lab.
- All students must abide by the IT Policy and Procedure.
- Violation or abuse of any policy, equipment, or computer lab will be reported to Safety & Security and the Dean of Student Services. It may result in suspension or revocation of lab privileges.
- All users should have a personal data disk or flash drive to save their work or utilize their CMI student Google drive storage. Will delete any files or not approved software found on the hard drive. The IT Department is not responsible for unsaved data lost due to power failure, computer failure, or other unplanned or unavoidable events or emergencies.
- **NO** Cyber Bullies

6. Cross References to Related Policies and Regulations

HR Policy and Procedure Handbook, Student Handbook, & FERPA (external link to the USA government FERPA website)

7. Responsible Office

Director, Information Technology

8. Key Offices to Contact Regarding the Policy and its Implementation

Information Technology Department

Date of Initial Policy:
October 29, 2004

Date(s) of Any Revision:

- Approved by the Board of Regents on October 29, 2004,
- Revised and Recommended for Approval by the Executive Council May 2008
- Approved by the Executive Council on April 19, 2013,
- Approved by the Executive Council on February 5, 2016,
- Approved by the Board of Regents on September 21, 2016,
- ITC Ad-hoc Committee review on February 15, 2022,
- Approved by the ITC on April 6, 2022,

1st reading by the Ad-hoc committee: 2/15/2022
2nd reading by ITC 2/22/2022
Approved by ITC 4/6/2022 (Email approved)
Approved by EC_07/22/2022

CMI POLICY NO. 640.02

Series 600: General Administrative Policies
Section 640: Other Policies
Computers, Email, Internet, Network, Communication, & Physical Facilities
Status:
Effective Date:
Steward:
Approval Authority:

1. Policy Statement

This Policy Statement provides notice of the college's expectations and guidelines to all who use and manage Information Technology resources and services (including but not limited to computer, Email, Internet, Network, Telephone, and Physical facilities.

2. Reason for the Policy

CMI has created this policy to maximize the benefits of its computer resources and minimize potential liability. All computer users must use these resources responsibly, professionally, ethically, and lawfully. Users must not present false identification or misleading information to access computing resources or use them for which they are not authorized.

3. Definitions

Email Systems:

The College of the Marshall Islands' email system (Google Workspace for Education) supports the college's educational and administrative activities. It serves as a means of official communication by and between the users and the college. The purpose is to ensure that important service remains available, reliable, and used for appropriate purposes. The college provides email services to faculty, staff, and students, including official visitors. Finally, the college may also offer an email service to CMI alumni. The use of college email services must be linked with the college's educational goals and comply with all applicable laws and college policies.

Only full-time employees and students are authorized users entitled to use the email services. All employees and students of the college who agree to and abide by the College Policies and procedures are allowed to use the facilities and email services when the system is available. The Information Technology Department is responsible for providing and maintaining email systems.

Internet & Network Service:
Using the Internet for CMI business purposes (including research, course development, etc.) is a necessary benefit for employees. Personal use of the internet should be kept to a minimum. Inappropriate use of the internet is prohibited. Unacceptable use includes such activities as viewing sexually explicit sites, conducting or participating in any activity that threatens the college's tax-exempt status, and activities deemed illegal in the Republic of the Marshall Islands. Internet access provided by the college to every user and managed by the IT Department shall enjoy the same privileges and be subject to the same restrictions, guidelines, and procedures. Use of the college's internet for personal use during working hours should be kept to a minimum and is subject to the policies and all associated rules outlined in this and other College policies, statutes, and bylaws.

Telephone System-
The information technology department supplies most telecommunications equipment for use by departments. IT Department operates in a manner designed to recover most costs for equipment and services provided. The requesting Department will shoulder the telephone equipment fee out of their budget. The college acknowledges that a limited number of personal local phone calls made during working hours are necessary for employees; however, such calls should be kept to a minimum. This applies to all CMI staff, faculty, and students. Every user will have their PIN code for a long-distance call. If an employee makes personal long-distance phone calls, that employee must pay for all charges associated with the rings. Employees are not allowed to share the PIN code with others. The PIN code's owner will be held responsible for any misuse of the calls.

4. Statements of Elaboration of Policy

The computer, systems, and network belong to CMI and should be used for CMI business or academic purposes. All Information Technology resources may not be used for personal business. The college may review any material created, stored, sent, or received on its network, through the Internet, or any other computer network.

5. Procedures

Unacceptable Use of Email

The primary purpose of the email is to support the college's teaching, learning, research, and official business activities; inappropriate use of the college's email includes, but is not limited to

- Unauthorized and intentional access to people's email accounts without the consent of the users.
- Messages or transmitting illegal material.

- The transmission of unsolicited emails not related to College affairs.
- Send messages that constitute violations of the College's Student Conduct Code or Human Resources Policy and Procedure Handbook.
- Creation and use of a fraudulent or alias email address to impersonate another or send fraudulent communications;
- Directly or indirectly impeding the college's operation of email services.

The college permits email services for employees and other authorized users for personal use so long as they do not constitute inappropriate use (see section Acceptable Use of Email.). Students, staff, and faculty shall not give the impression that they represent, offer views, or otherwise make opinions and decisions on behalf of the college or any unit unless appropriately authorized explicitly or implicitly.

Acceptable Uses of email services

- Employees accessing email represent the college. All communications should be for professional reasons. Employees and students are responsible for ensuring that email is used effectively, ethically, and legally. Process-enabled access to email database/s of which information is only intended for law enforcement, legal, or court proceedings shall be acceptable.
- Each student and employee is responsible for the content of all text, audio, or images they place or send over an email and the internet. Fraudulent, harassing, or obscene messages are prohibited.
- All messages communicated by email should have a sender's name, whether a single user's name or a recognized and approved group email address. No email will transmit under an assumed representation.
- Users may not attempt to conceal the origin of any message. Information published in emails should not violate or infringe upon the rights of others.
- No abusive, profane, or offensive language will be transmitted through the system. Students and employees who wish to express personal opinions must use non-College email and Internet systems.
- All messages created, sent, or retrieved over email are the college's property and should be considered college information. The college reserves the right to access and monitor all messages and files on the computer as deemed necessary and appropriate.
- All information and data communication, including text and images, can be disclosed to law enforcement or a third-party company without the prior consent of the sender or receiver.

Violations of any guidelines listed here may result in disciplinary action up to and including termination.

Termination of Email & Other Accounts-

- When an **employee** leaves the college, the email account is terminated upon signing the HR clearance form. The employee must back up and transfer all data and personal information to their email accounts before the IT Director signs the clearance form.
- When **students** graduate from college, they can continue to access their CMI email account as an alumnus. The standard email address shall be set to the "johnjoe@almuni.cmi.edu email domain." The email address shall be suspended for students who are not registered in the current semester and are considered inactive. The email address shall be reactivated once they become active CMI students again.

Incident report (Email & Systems) Data Protection,

The IT Department of the College will investigate complaints from internal and external sources about the unacceptable use of email services and other college-used technology systems. In concurrence with other departments as appropriate, the IT Department will collate information from a technical perspective. An ad-hoc committee shall convene to further look into the incident, and the members shall include Faculty, Staff, and Student Conduct Committee representatives.

Bulk Email Policies and Procedures

Bulk emails communicate important academic and college work-related information announcements to students, faculty, and staff. This procedure must be read and shared with the college community before utilizing the bulk distribution list on the email system.

Specifically, the bulk emails should not be used for:

- Emails not related to college business affairs or activities
- Emails in violation of IT Policies and Procedures
- Emails are associated with any political statements, expression of personal opinions, and conduct of private business.
- Unauthorized fundraising or solicitation through the sale of merchandise/services or charitable donations and influence opinions or gain support for an issue.

- Repeated Messages: Sending multiple versions of the same message, either as a reminder, follow-up, or correction for inaccurate information. (Review the statement very carefully before sending them).

Guidelines and Criteria

The use of email abides by the College IT Policies and Procedures Manual. Email sent out in bulk to the community is the employee's responsibility. Users who want to send emails to the college's approved mailing list must abide by the following guidelines. The Bulk Email is appropriate for

- Announcements of campus-sponsored events
- Announcements of official policies or changes in policy or procedures
- Announcements of disruption of services (i.e., electrical/power disruptions, campus network/internet outages, Network upgrades, registration changes, etc.)
- Announcements from the standing committee.
- Announcements that notify and alert the community of health and safety issues.
- Messages inform and alert the community of any significant events or changes in government, policy, and practice.
- Messages inform the community or events related to academic events, such as student classes and related announcements within the college.

Violating these procedures will result in a temporary suspension of bulk email messages; the first violation is a warning and a second violation results in a semester suspension. All violations are initially determined by the Information Technology Department but can be appealed to the IT Committee.

To report a bulk email violation of this procedure, please contact or write to abuse@cmi.edu.

Any bulk email sent to the college-wide official announcement or another mailing list must have approval from the designated moderators. The message will not be directly delivered to anyone's mailbox until the moderator approves it. An E-requests will not be accepted or approved if they do not meet the requirements.

Authorizations and Approvals

Mailing List	Moderators
cmicom@cmi.edu	SLT

1st reading by the Ad-hoc committee: 2/15/2022
2nd reading by ITC 2/22/2022
Approved by ITC 4/6/2022 (Email approved)
Approved by EC_07/22/2022

stucom@cmistudent.com **announcement@cmistudent.com**	**Dean & Associate Dean of Equity & Engagement**
All Standing Committees	**No moderators**

Acceptable Internet Use Policy

Using the Internet for CMI business purposes (including research, course development, etc.) is a necessary benefit for employees. Personal use of the internet should be kept to a minimum. Inappropriate use of the internet is prohibited. Unacceptable use includes such activities as viewing sexually explicit sites; conducting or participating in any activity that threatens the college's tax-exempt status and activities that are deemed illegal in the Republic of the Marshall Islands;

Internet access provided by the college to every user and managed by the IT Department shall enjoy the same privileges and be subject to the same restrictions, guidelines, and procedures. Use of the college's internet for personal use during working hours should be kept to a minimum and is subject to the policies and all associated rules outlined in this and other College policies, statutes, and bylaws.

Internet Unacceptable Use Policy,

Unacceptable uses of the college's internet resources, which shall amount to a violation of this policy, shall enclose, but not be limited to, the following:

- Any illegal activity, including cybercrimes.
- For any political purpose.
- To access, share or download sexually explicit or obscene material.
- To access online gambling sites.
- To defame any person or create liability for the college.
- Any malicious attempt to damage, modify, and destroy the data of another user, internet, or other networks connected to the Internet backbone, such as uploading or creating computer viruses, intentionally disrupting network traffic, or crashing network and connected systems.

Internet access provided by the college is a privilege, not a right. It is only for academic & college business purposes. Unacceptable use may cancel the privilege, including violating these conditions and rules.

Computer Systems (Ownership of Software and Hardware)

All software and files on CMI computer systems are the college's property. The college reserves the right to inspect/delete/print files, software, and user accounts. Moreover, the college reserves the right to revoke computing privileges to any user. Unless extenuating circumstances prevent, users shall receive timely, transparent, and complete notification before any such action is taken. All computers issued to staff and faculty are the college's property.

The college may provide computer or computing devices or similar equipment to Employees (Faculty and Staff) to perform job functions such as academic instruction, research, business operations, and other duties as set forth by the sole discretion of the college. Each employee receiving any devices must read and sign this Policy and Procedure upon receipt of equipment.

Employee Responsibilities:

1. Employees are assigned a laptop or desktop and similar devices to perform duties directly related to the business of CMI. Laptops/mobile devices shall not be used by non-employees and are not intended for any non-College business.
2. All users are responsible for all data stored on the hard drive of a laptop or desktop computer in terms of security backup. The IT Department recommends saving all files to Google Drive for security purposes.
3. Employees' use of College equipment or devices shall strictly adhere to the College's IT Policy and Procedure Manual.
4. In most circumstances, laptop and desktop devices will install a standard suite of approved software and security apps installed by the college. An employee shall not modify or disable these software or security applications without written approval from the IT Department.
5. All laptops and desktop computers connected to the local network must join College Domain controller services.
6. College standard covers college laptops and desktop devices warranty, replacing defective hardware parts. This warranty does not cover drops, falls, electrical surges, liquids, spilled units, fire damage, intentional damage, everyday wear, tear, lost parts (power units), or consumables (batteries). In the event of damage or malfunction, the employee must return the equipment within two (2) business days to the IT Department for repair or replacement.

7. In the circumstance of theft of college-issued equipment, the employee shall immediately notify their supervisor and the IT Department. If the college requires it, the employee must file a police report and provide a copy of the information to their superior.
8. Employees are responsible for taking reasonable precautions to protect and maintain the college's laptops and desktop devices.
9. Evidence of misuse or abuse of a computer may result in the revocation of the employee's use of such equipment or device. Furthermore, employees may be responsible for the loss of value associated directly with intentional misuse or abuse.
10. If an employee's employment ends at college, they shall return the equipment no later than their last day of work.
11. The college provides computer replacement upgrades every three years for laptop users and five years for desktop computers. Refer to ***Equipment Replacement Procedure***

Web Posting Procedures

The purpose of the Web Posting Procedure is to ensure consistency, completeness, and compliance with the college branding guidelines and standards for the advancement of the CMI website. The College Community recognizes the CMI website *(www.cmi.edu)* as an effective resource for recruitment practical and marketing tools to attract potential candidates/students, disseminate students' news, and communicate with external stakeholders/audiences, including potential students and the community at large

The following are allowed to submit content to be posted on the CMI website.

- Board of Regent
- CMI Employee (Staff, Faculty, Administrators)
- CMI Student (must be officially enrolled)

Content authors are responsible for ensuring that their content is up to date and report any outdated material needs to be removed.

Content Visibility

Content published on the website is public unless specified by the user. Documents shall be uploaded to the Document Management System (eFilecabinet) of the College or the media library of the content management system.

Review

The Website Committee shall review the website at least once every academic year. The Website Committee shall provide the IT Committee with a recommendation if maintenance is necessary and a significant update.

Copyright

CMI assumes that the author rightfully owns any content submitted for posting. If a piece of content is a copyrighted work, they must be authorized to use or reproduce it to avoid copyright infringement. Copyrighted works include but are not limited to text, images, videos, graphics, records, audio, or software programs.

CMI assumes no responsibility for individual failure to fulfill this or other legal obligations. Any comments and feedback should be addressed to the owner of the content.

Any content (pages, articles, and images) that violates this policy will be unpublished and removed. The content owner shall be informed, and the issue shall be addressed accordingly.

Web Posting Guidelines

Content Management Access

The Information Technology Department provides access to the website's content management through a written request that will be evaluated based on the following criteria:

- Level of access
- Requestor's position
- Requestor's familiarity with the content management system

Content Submission

The client, any stakeholder authorized to submit content and approved by the immediate supervisor or Department Head, should send the request to IT Department. IT personnel will validate the request based on the following criteria:

- **Quality of the content**
  - The material should be curated with purpose and correct grammar.
  - Content may not contain non-CMI advertising, except with the permission of the corresponding Vice President or President of CMI.
- **Validity**
  - The content shall be accurate and up to date.
- **Legality**
  - The content shall not violate any law or policy, including but not limited to: copyright, harassment, libel, or obscenity.

1. If the request is invalid, the IT personnel will provide feedback to the client.
2. Once the request is deemed valid, the assigned IT personnel will work on it and provide client feedback once it is considered good. Once the request is fulfilled, the information will be posted on the college's website. Otherwise, the client will provide the necessary input and send the information back to the IT department until the request is satisfied. Refer to the *Web Posting Procedures Flowchart*

CMI reserves the right to change this procedure at any time. CMI will post the most up-to-date, approved version of the policy on CMI's website and may, at its discretion, provide users with additional notice of significant changes.

1st reading by the Ad-hoc committee: 2/15/2022
2nd reading by ITC 2/22/2022
Approved by ITC 4/6/2022 (Email approved)
Approved by EC_07/22/2022

6. Cross References to Related Policies and Regulations

HR Policy and Procedure Handbook, Student Handbook, & FERPA (external link to the USA government FERPA website)

7. Responsible Office

Director, Information Technology

8. Key Offices to Contact Regarding the Policy and its Implementation

Information Technology Department

Date of Initial Policy:
October 29, 2004

Date(s) of Any Revision:

- Approved by the Board of Regents on October 29, 2004
- Revised and Recommended for Approval by the Executive Council May 2008
- Approved by the Executive Council on April 19, 2013
- Approved by the Executive Council on February 5, 2016,
- Approved by the Board of Regents on September 21, 2016,
- ITC Ad-hoc Committee review on February 15, 2022
- Approved by the ITC on April 6, 2022

CMI POLICY NO. 640.03

Series 600: General Administrative Policies Section
Section 640: Other Policies

Copyright Law

Status:
Effective Date:
Steward:
Approval Authority:

1. Policy Statement

This copyright policy applies to all college employees and students and should follow the supporting information in the HR Policy and Procedure Handbook and Student Handbook.

2. Reason for the Policy

All college employees are expected to respect the copyright associated with intellectual property, which, except under limited circumstances, prohibits the duplication, public display, or performance of such property without permission of the owner of that copyright

3. Definitions

Third-party copyright- is when the rights to the material belong to someone other than yourself, such as images and extended text citations. If you are using material like this in your work, you will need to seek permission from the people or company that owns the rights before using it.

Intellectual property includes visual images, software, applications, and other creative expressions, whether fixed electronically or hard copy. Copyright law is a significant part of the academic community's legal framework *(Refer to **HR Policy and Procedure Handbook**)*.

4. Statements of Elaboration of Policy

An integral part of the free exchange recognizes the intellectual property work of others, honest representation, and the rights of others. It includes the instructor's and fellow students' right to intellectual property in their lectures, notes, slides, and other course-specific materials and the right to limit the distribution of images and recordings of oneself.

5. Procedures

Ownership and Use

The college will assert ownership rights to intellectual property developed under the following circumstances:

- If the college funded or sponsored the research program
- If it is required to use significant College resources.
- The creator was assigned, directed, or specifically funded by the college to develop the materials.
- Any materials developed by the employees during their terms of employment duties constitute the work-hire contract.

Learning Management System

The LMS hosts content and courses. It provides an online, accessible platform to deliver to users for academic purposes. Any systems created by the content creator are not allowed to be duplicated or copied without the original course creator's consent and permission. If the initial course creator agreed to use their course, it is necessary to acknowledge them as its original owner.

College Employees must comply with all copyright laws and College policies and procedures governing software products' use. Unauthorized copying or disposal of the software shall be considered a violation of College policy. Procedures to manage the use of the college's strategies sources shall be maintained by the Information Technology Department.

6. Cross References to Related Policies and Regulations

HR Policy and Procedure Handbook, Student Handbook, & FERPA (external link to the USA government FERPA website)

7. Responsible Office

Director, Information Technology

1st reading by the Ad-hoc committee: 2/15/2022
2nd reading by ITC 2/22/2022
Approved by ITC 4/6/2022 (Email approved)
Approved by EC_07/22/2022

8. Key Offices to Contact Regarding the Policy and its Implementation

Information Technology Department

Date of Initial Policy:
October 29, 2004

Date(s) of Any Revision:

- Approved by the Board of Regents on October 29, 2004,
- Revised and Recommended for Approval by the Executive Council May 2008
- Approved by the Executive Council on April 19, 2013,
- Approved by the Executive Council on February 5, 2016,
- Approved by the Board of Regents on September 21, 2016,
- ITC Ad-hoc Committee review on February 15, 2022,
- Approved by the ITC on April 6, 2022,

1st reading by the Ad-hoc committee: 2/15/2022
2nd reading by ITC 2/22/2022
Approved by ITC 4/6/2022 (Email approved)
Approved by EC_07/22/2022

CMI POLICY NO. 640.04

Series 600: General Administrative Policies Section
Policy 640- Ethical Standards, Data Privacy, & Responsibilities
Status:
Effective Date:
Steward:
Approval Authority:

1. Policy Statement

The college has developed the following policy regarding ethical standards in using computing systems at CMI. Computing systems exist for the constructive use of information. Students, faculty, and staff should be guided by prevailing principles that govern other processes and academic treatments at CMI.

2. Reason for the Policy

Data Privacy, Confidential, and Restricted Information

Data privacy is confidential and restricts information since CMI values the individual's privacy. The cloud storage and central repositories are categorized to ensure that sensitive data is limited to those with a legitimate educational or with business-related purpose for using it. The highest level of sensitivity, confidential information, is defined as information that could cause substantial damage to or liability for CMI if treated imprudent.

3. Definitions

All types of recorded information and access to that information by written, oral, and visual, in any media, including paper and electronic, shall be protected. The external dissemination of confidential and restricted information, including electronic and paper, shall be limited regardless of the media. Safeguarded precautions shall be utilized when providing information in electronic form or other media.

4. Statements of Elaboration of Policy

Transmitting sensitive or confidential information via email without proper safeguards is not permitted unless the sender must use the confidential mode features of the email system. If employees are unsure about what indicates acceptable IT policy and procedures usage, they should ask their supervisor for further guidance and clarification.

1st reading by the Ad-hoc committee: 2/15/2022
2nd reading by ITC 2/22/2022
Approved by ITC 4/6/2022 (Email approved)
Approved by EC_07/22/2022

5. Procedures

The students, faculty, and staff should consider issues such as courtesy and good taste and those of pure legality. Use of computer resources for any of these activities is strictly prohibited:

- Use of an unauthorized computer account.
- Introduce malicious software onto the company network and jeopardize the security of the college's electronic communications systems.
- Interfere with the regular operation of computers, terminals, peripherals, or networks.
- Giving another user a program intended to damage or place excessive load on a computer system or network includes, but is not limited to, programs and applications known as computer viruses. Attempt to bypass data protection schemes or uncover security vulnerabilities.
- Violate terms of applicable licensing agreements.
- Use of electronic mail to harass others or colleagues.
- Post materials on electronic bulletin boards/portals that violate applicable laws or college policies.
- Attempt to monitor or meddle with a user's electronic communications or copy, read, change, or remove another user's files without the owner's explicit permission.
- Use college resources for commercial purposes or personal financial gain.
- Use college resources for the creation or distribution of unauthorized promotional materials.
- Activity violates any college policies, including but not limited to the college's non-discrimination policy, sexual harassment, or gender discrimination.
- It is downloading, reproducing, copying, and pirating software and electronic files that are copyrighted or without authorization.
- Use of computing resources in such a way as to hide the identity of the user or poser users

If you know someone using computer resources for these activities, you must immediately report the incident to the IT Department. Violations of this IT Policy may result in reprimand. They may result in disciplinary action, including suspension of privileges, possible employment termination or college expulsion, and civil and criminal liability.

The college adopts an educative approach to copyright by providing support services and materials that inform practice for employees and students.

6. Cross References to Related Policies and Regulations

HR Policy and Procedure Handbook, Student Handbook, & FERPA (external link to the USA government FERPA website)

The college must follow Family Educational Rights and Privacy Act (FERPA) which covers student education records and information.

FERPA (external link to the USA government FERPA website)

Restricted information and communication are defined by the need for special protection beyond that taken for public information. All information in this procedure includes the secure transmission and removal of data or information technology. Communication released to the public must go through the Community Liaison Officer according to guidelines developed to safeguard the information.

7. Responsible Office

Director, Information Technology

8. Key Offices to Contact Regarding the Policy and its Implementation

Information Technology Department

Date of Initial Policy:
October 29, 2004

1st reading by the Ad-hoc committee: 2/15/2022
2nd reading by ITC 2/22/2022
Approved by ITC 4/6/2022 (Email approved)
Approved by EC_07/22/2022

Date(s) of Any Revision:

- Approved by the Board of Regents on October 29, 2004
- Revised and Recommended for Approval by the Executive Council May 2008
- Approved by the Executive Council on April 19, 2013
- Approved by the Executive Council on February 5, 2016,
- Approved by the Board of Regents on September 21, 2016,
- ITC Ad-hoc Committee review on February 15, 2022
- Approved by the ITC on April 6, 2022

All terms and conditions expressed in this document apply to all users. The terms and conditions stated on this document reflect the employee and the college's agreement. It should be governed and interpreted following the above-mentioned policies and procedures and other college policies (***HR Policy and Procedure Handbook, Student Handbook).*** *Any user violating these policies is subject to disciplinary actions deemed appropriate by the college.*

Violations

When any use of information technology at the college presents an imminent threat to other users or the college's technology infrastructure, IT Department personnel may take whatever steps necessary to isolate the danger without notice if circumstances require. This may include changing passwords, locking files, disabling computers, or disconnecting specific devices or entire sub-networks from the main campus or Centers.

A violation of this policy is deemed a breach of the College's Mission, Visions, and Values. Relying on the severity of the conduct, it also may violate the college's other policies or local law. The college may impose penalties ranging from the termination of the user's access to the Information Technology Resources to disciplinary review and non-reappointment, discharge, or dismissal. In cases involving apparent violations, the college may institute legal action lawsuits broughat the college may initiate legal action lawsuits brought by relevant authorities or third parties. In cases involving apparent violations against the students can refer to the **Student** ***Handbook***.

The employee is subject to disciplinary action, including reprimand, suspension, and dismissal, as stipulated in the ***HR Policy and Procedure Handbook.***

Depending on the nature and severity of the violations, sanctions can range from various levels of warnings to immediate termination of employment for (employee) and enrollment (students).

The college will express good faith in its enforcement of this policy. It will respect the *academic freedom* to which users are entitled to the extent of the legal rights and obligations of the College permit.

Under no circumstances shall the college be held responsible to any User or Guest for any violation, including illegal or improper acts that any users commit using the College's IT Resources.

1st reading by the Ad-hoc committee: 2/15/2022
2nd reading by ITC 2/22/2022
Approved by ITC 4/6/2022 (Email approved)
Approved by EC_07/22/2022

User compliance

I understand and will abide by the IT Policy and Procedure. I further understand that should I violate this policy, my access privileges may be revoked, and disciplinary action and appropriate legal action may be taken.

___________________ ________________

Employee signature Date

1st reading by the Ad-hoc committee: 2/15/2022
2nd reading by ITC 2/22/2022
Approved by ITC 4/6/2022 (Email approved)
Approved by EC_07/22/2022