Maria College

Computer Use Policy

1. Overview

Maria College's intentions for publishing a Computer Use Policy are not to impose restrictions that are contrary to Maria College's established culture of openness, trust, and integrity. The College is committed to protecting our faculty, staff, student, and the College from illegal or damaging actions by individuals, whether done knowingly or unknowingly. Systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts, electronic mail, web browsing, are the property of Maria College. These systems are to be used in serving the interests of the college, and of our students in the course of normal operations.

Effective security is a team effort involving the participation and support of every Maria College employee and student who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer resources at Maria College These rules are in place to protect the employee, student, and the college. Inappropriate use exposes the College to risks including virus attacks, compromise of network systems and services, loss of records, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources used to conduct Maria College business and/or to interact with internal and external networks and business systems, whether owned or leased by the College, the employee, the student, or a third party. All employees, contractors, consultants, temporary and other workers, and students at Maria College and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Maria College's policies and standards, as well as local, state or federal laws and regulations. This policy applies to employees, contractors, consultants, temporary and other workers, and students at Maria College including all personnel affiliated with third parties. This policy applies to all resources that are owned or leased by the College or licensed to the College.

4. Policy

4.1 <u>General Use and Ownership</u>

4.1.1 Maria College's proprietary information stored on electronic and computing devices whether owned or leased by the college, the employee, or a third party whether the data is stored on campus or at a third-party location remains the sole property of the College.

4.1.2 You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Maria College proprietary information.

4.1.3 You may access, use, or share Maria College proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Employees and students are responsible for exercising good judgment regarding the reasonableness of personal use of Internet/Intranet/Extranet systems.

4.1.5 For security and network maintenance purposes, authorized individuals within Maria College may monitor equipment, systems and network traffic at any time.

4.1.6 Maria College reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2. Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.

4.2.2 System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3 All computing devices must be secured with a password-protected locked screen with the automatic activation feature set to 30 minutes. You must lock the screen or log off when the device is unattended.

4.2.4 Postings by employees and students from a Maria College email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Maria College, unless posting is in the course of business duties.

4.2.5 Employees and students must use extreme caution when opening e-mail attachments, which may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees and students may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee or student of Maria College authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing College-owned or -leased resources. The lists below are by no means exhaustive, but provide a framework for activities which fall into the category of unacceptable use.

4.3.1 *System and Network Activities*

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including but not limited to the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Maria College.

- Unauthorized copying of copyrighted material, including but not limited to digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Maria College or the end-user does not have an active license is strictly prohibited.

- Accessing data, a server, or an account for any purpose other than conducting Maria College business, even if you have authorized access, is prohibited. Accessing the email account of any person other than yourself, whether it is the account of a student or an employee, is absolutely prohibited unless explicit permission to do so is granted by the College President and a clear, legitimate Maria College business purpose for the access exists. In instances that involve the email account of the President, explicit permission must be obtained from the Chair of the College Board of Trustees. College officials who seek such access must first seek authorization from the appropriate College official by submitting and provide reasons in support of the request. Legitimate reasons for which Maria College may grant access include but are not limited to: maintaining the system, preventing or investigating allegations of system abuse or misuse, assuring compliance with software copyright laws, complying with legal and regulatory requests for information, and ensuring that College operations continue appropriately during an employee’s absence.

- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

- Using a Maria College computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

- Making fraudulent offers of products, items, or services originating from any Maria College account.

- Effecting security breaches or disruptions of network communication. Security breaches include but are not limited to accessing data for which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes but is not limited to network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

- Port scanning or security scanning is expressly prohibited unless prior notification to the Information Technology Office is made.

- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

- Circumventing user authentication or security of any host, network, or account.

- Introducing honeypots, honeynets, or similar technology on the Maria College
  Network unless is within the normal scope of job duties network.

- Interfering with or denying service to any user other than the employee's host
  (for example, denial of service attack).

- Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session via any means, whether locally or via the Internet/Intranet/Extranet.

- Providing information about and/or lists of Maria College employees to parties outside the college.

4.3.2 *Email and Communication Activities*

When using College resources to access and use the Internet, users must realize they represent the College. Whenever employees state an affiliation to the College, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the College". Questions may be addressed to the IT Department. The following activities are strictly prohibited, with no exceptions:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

- Any form of harassment via email, social media, telephone, or paging, whether through language, frequency, or size of messages.

- Unauthorized use, or forging, of email header information.

- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

- Creating or forwarding "chain letters", "Ponzi", or other "pyramid" schemes of any type.

- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.3.3 *Blogging and Social Media Posting*

The following policies apply to blogging and social media activities:

- Blogging or posting by employees or students, whether using Maria College's property and systems or personal computer systems, is subject to the terms and restrictions set forth in this policy. Limited and occasional use of Maria College's systems to engage in blogging or posting is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate the College's policies, is not detrimental to the College's best interests, and does not interfere with an employee's regular work duties. Blogging or posting from Maria College's systems is subject to monitoring.

- Maria College's Confidential Information Policy applies to blogging and/or posting. As such, employees and students are prohibited from revealing any confidential or proprietary information, trade secrets, or any other material covered by Maria College's Confidential Information policy when engaged in blogging or posting.

- Employees and students shall not engage in any blogging or posting that may harm or tarnish the image, reputation, and/or goodwill of Maria College and/or any of its employees or students. Employees and students are prohibited from making any discriminatory, disparaging, defamatory, or harassing comments or otherwise engaging in any conduct prohibited by the college's Non- Discrimination and Anti-Harassment policy when blogging or posting.

- Employees and students may not attribute personal statements, opinions, or beliefs to Maria College when engaged in blogging or posting. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the College. Employees and students assume any and all risk associated with blogging or posting.

- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Maria College's trademarks, logos, and any other Maria College intellectual property may not be used in connection with any blogging or posting activity.

5. Policy Compliance

5.1 Compliance Measurement

The Information Technology team will verify compliance to this policy through various methods, including but not limited to business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Director of Information Technology in advance.

5.3 Non-Compliance

An employee or student found to have violated this policy may be subject to disciplinary action, up to and including dismissal.

Email Disclaimer

This message is intended only for [recipient name]. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

Maria College accepts no liability for the content of this email, or for the consequences of any actions taken on the basis of the information provided. Any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the college.

Logon Screen Policy Acknowledgement

This computer system is the property of the Maria College. It is for authorized use only. By using this system, all users acknowledge notice of, and agree to comply with, the College’s Computer Use Policy. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use.

If you do not agree to these conditions as stated, **DO NOT CONTINUE TO LOG ON.**