Maria College
Computer Use Policy

1. Introduction

   Maria College's Computer Use Policy provides guidance that is in alignment with Maria College's established culture of openness, trust, and integrity. The College is committed to enable effective use of technology resources while protecting our faculty, staff, students, and the College from illegal or damaging actions by individuals, whether done knowingly or unknowingly. 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 be aware of and understand these guidelines, and to conduct their activities accordingly.

2. Overview

   The purpose of this policy is to outline the acceptable use of computer resources at Maria College. When referenced in this document, "Maria College authorized users" include faculty members, staff and enrolled students.

   The provisions outlined are in place to protect the employee, student, and the College. Inappropriate computer use exposes the College to risks which may include virus attacks, compromising of our network systems and services, loss of records (including personal data), and legal issues.

   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 or external network and other systems that are owned or leased by the college, an employee, student or third party. All employees, contractors, consultants, temporary workers and students at Maria College are responsible for exercising good judgment regarding the appropriate use of information, electronic devices, and network resources in accordance with Maria College's policies as well as local, state, and federal laws and regulations.

3. General Use, Ownership and Responsibility

   Maria College's proprietary information is the sole property of the College. This includes information stored on electronic devices regardless of whether the device is owned or leased by the college, employee or third party and regardless of whether the data may be stored on or off campus.

   Under no circumstances is an employee or student at Maria College allowed to engage in any activity that is illegal while using a college owned or leased device.

   All Maria College authorized users:

   - Have a responsibility to promptly report the loss, theft or unauthorized use of Maria College information or equipment.

- May be granted permission to access, use or share Maria College information only to the extent it is necessary to fulfill assigned job duties.
- Are responsible to exercise good judgment in their use of the internet. Internet use should be limited to business and academic activities related to Maria College business. Individuals should not download and/or install any software from the internet or other media.

4. Privacy

Privacy and the expectation of privacy are very important aspects of human dignity; however, it is also important that the institution may need access to an employee's email or hard drive to conduct its business. There is a need to be clear about who may authorize access to an employee's electronically stored information, and what safeguards are in place to prevent misuse of the emails and information once accessed. Only the president, the board chair, or their designee, may authorize access to anyone else's email or hard drive (without the individual's permission) and only for specific business-related purposes. Beyond the information concerning the specific purposes for which they were granted access, the individual who is granted such access may not share any other information acquired by their access with anyone, The sole exception is if the information discloses a danger to others, or actual or planned criminal conduct, in which case they should share only with the president who will consult with legal counsel and/or law-enforcement.

5. Data Security and Integrity

Maria College IT Department recommends Microsoft One Drive for the storage of data files. Files may also be stored on network shares (ex. User folders). Both systems are routinely backed up. Your email account should not be used as data repository. In no circumstances should a personal cell phone or unauthorized backup drive (USB/Flash drive) be connected to the college network or equipment.

Files that are saved on an individual device desktop or C Drive are not backed up.

All computing devices are secured with a password-protected locked screen which will automatically be activated within 30 minutes if the device is unattended.

All Maria College authorized users:

- Are responsible for safeguarding their system access login and password credentials. Passwords must meet the complexity requirements outlined and must not be shared. The following parameters indicate the minimum requirements for passwords:
    - At least fourteen (14) characters
    - At least one uppercase letter
    - At least one lowercase letter
    - At least one number
    - At least one symbol

Passwords will expire 6 months after the date you set/reset the password. Some administrative accounts expire 3 months after the date you set/reset the password.

Maria College makes use of Single Sign On for ease of access to applications and Multi Factor Authentication to increase security.

- Should be careful not to open unexpected or unsolicited attachments from unknown or even known senders, nor follow web links within an email message unless the user is certain that the link is legitimate. Following a link in an email message executes code, that can also install malicious programs on the computer.
- Should notify IT staff immediately in the event of data loss or corruption. Every reasonable attempt will be made to restore files.
- Should only access data files, equipment, servers or an account for which they are authorized and have a legitimate business purpose.

All Maria College faculty and staff will adhere to the Confidentially Policy that is on file and available upon request.

In addition, the IT Office will adhere to the Computer System Administrator IT Policy on file and available upon request. System Administrators/members of the IT staff are forbidden to log on to a user account or to access a user's files unless the user gives explicit permission.

6. Appropriate Computing Behavior

All Maria College authorized users who use campus technology or network computing resources are required to behave in a manner consistent with Maria College's code of conduct. The College supports computing activities which promote research and learning by the user of the computer systems.

All Maria College authorized users:

- Should be sensitive to the nature of shared facilities and take care not to display on screens in such locations images, sounds or messages which could create an atmosphere of discomfort for others. You must also refrain from transmitting to others inappropriate images, sounds or messages which might violate the College's statements on harassment.
- Are provided with various software applications for their sole use only. No attempt should be made to copy or make use of these applications in an unauthorized manor.
- Should not use Maria accounts, credentials or equipment to post on social media unless it directly relates to Maria activities. This includes restrictions for creating or sending chain letters, junk mail, or unwanted advertising.

7. Policy Compliance

Violations of the Computer Use Policy are treated like any other ethical violation as outlined in the Student Handbook, relevant third-party contractual agreements, and applicable faculty and staff handbooks. Penalties may include but are not limited to the restricting or potential suspension of access as is deemed necessary by the College.

Any variation or exception to the Computer Use Policy must be approved in writing by the Director of Information Technology in advance.

The Information Technology staff will verify compliance to this policy through various methods, including but not limited to business tool reports, direct observation, internal and external audits, and feedback to the Director of IT.