Responsible Use of Information Technology

Revised July 2016

Access to Mount St. Joseph University's electronic mail (email), internet, electronic files, and any other information technology (IT) systems are provided by the University for the benefit of students, faculty, staff and the University. Access to such systems is a privilege and must be used responsibly. Although the University does not intend to monitor the content of electronic mail, internet use, or electronic files as a routine procedure, the University reserves the right to access, inspect, copy, transfer, store, or disclose the contents of electronic mail messages, internet data transmissions, and electronic files when appropriate. It may be appropriate to access, inspect, copy, transfer, store or disclose the contents of such information in a variety of circumstances, including, but not limited to: preventing or correcting improper use of University E-Mail or IT systems; performing routine maintenance or system upgrades; ensuring compliance with University policies, procedures, expectations or regulations; ensuring compliance with applicable local, state and federal laws or satisfying other obligations; or ensuring the proper operations of University email and IT systems. Students, faculty and staff understand they have no expectation of privacy in connection with their use, storage, or transmissions using the University's email or IT systems. Any MSJ administrator who believes such actions are necessary must first obtain the written approval of the appropriate administrative officer. This policy is subordinate to local, state and federal law. Violation of this policy may result in disciplinary action in accordance with University policy.

The University employs various measures to protect the security of its computing resources and users' accounts. However, users should be aware that the University does not and cannot guarantee such security. Furthermore, students, faculty and staff are advised to exercise caution when sending sensitive or FERPA-protected student information via email. Mount community members are prohibited from sharing their Mount password(s) with any other individual and are prohibited from using their Mount user ID and password to provide access to the Mount's computer network for other individuals. At the time of resignation or termination, employees must either forward to their supervisors all University-related information that they have stored in electronic format or give supervisors access to the information.

In addition, all users of the University's email and IT systems must also comply with the following:

1. Intentionally accessing, uploading, downloading, posting, emailing or otherwise transmitting unlawful and/or inappropriate information, profane, vulgar, threatening, defamatory, abusive, discriminatory, harassing or otherwise objectionable or criminal language in a public or private message is prohibited. Racially or ethnically offensive material is prohibited.

2. Materials that are obscene or sexually explicit including images, messages, cartoons, jokes and audio or video files is prohibited.

3. Material to be plagiarized is prohibited. Any computer code files or programs or repetitive requests for information designed to interrupt, destroy or limit the functionality of any technology equipment or the University network is prohibited.

4. Using the network or internet in a way that would violate any federal or state law, or the University's policy, including but not limited to the following is prohibited:

    a) Uploading and downloading copyrighted material or threatening material;

    b) Installing or using file sharing software;

    c) Spreading computer viruses;

    d) Attempting to gain authorized access to system programs or computer equipment and files, including attempts to override any fire walls or other security techniques on the network, including the use of proxy server;

    e) Using University technology for commercial purposes or financial gain;

    f) Vandalizing equipment, including but not limited to defacing, disassembling or destroying equipment, computers or network'

    g) Attempting to obtain and/or using any administrative passwords is expressly forbidden and will result in termination of privileges and disciplinary actions.

Irresponsible use of Mount St. Joseph's information technology may result in loss of your network privileges and may lead to disciplinary action up to and including suspension or dismissal as defined in the University's Student and Employee Handbooks.