# COMPUTER USE POLICY

## 1.0 Purpose and Summary

1. This document provides guidelines for appropriate use of the wide variety of computing and network resources at Methodist University. It is not an all-inclusive document. It offers principles to help guide authorized users in the appropriate use of Methodist University's technology and network resources while serving as a reference point.

2. Individuals using computer or network resources belonging to the Methodist University must act in a responsible manner, in compliance with law and University policies, and with respect for the rights of others using a shared resource in an ethical, moral, and legal manner. The right of free expression and academic inquiry is tempered by the rights of others to privacy, freedom from intimidation, harassment, cyberbullying, sexual harassment, protection of intellectual property, ownership of data, security of information.

3. The University reserves the right to modify and/or expand this policy at any time. Use of the Methodist University's computer and/or network resources by any person shall be implicit acceptance of the current policy, and all authorized users are held responsible for using Methodist University's computing and network resources in an ethical, moral, and legal manner and in a manner otherwise consistent with this policy.

## 2.0 Scope

This policy applies to all faculty, staff, students, contractors, guests, and anyone else using Methodist University's technology and network resources. This includes use both on campus and from a remote location off campus. It is every faculty, staff and student's responsibility to know and follow these policies.

## 3.0 Rights and Responsibilities

All users shall follow appropriate standards of civility and conduct and respect the feelings of others when engaged in communication. This means that all users will identify themselves and restrain from any behavior or communication that might be considered harassing, discriminatory, or in any way calculated to cause discomfort, cyberbullying, or embarrassment to readers or users of the communication. Users must also refrain from sending, receiving, or accessing pornographic materials.

## 4.0 Copyrights and License

1. All users shall abide by copyright laws in accordance with the Digital Millennium Copyright Act of 1998, as it currently exists or as it may be amended, modified and/or supplemented from time to time. Users may not engage in the unauthorized copying, distributing, altering or translating of copyrighted materials, software, music or other media without the express permissions of the copyright holder. This means that copying or use of programs or files that are not licensed to the user is forbidden. If you don't own a copy of a program, you cannot load it on any Methodist University computers/laptops. You cannot load multiple copies of programs for which you don't own multiple licenses. If any computer software is loaded on a Methodist University computer/laptop and no license can be produced for the software, the Computer Services staff will remove the software from the computer until such time as the user provides proof of a license. This will also be reported to the President, or user's Vice-President, as appropriate.

2. When the University is informed of copyright violations by the copyright holders or their representatives, we will comply with their requests to identify the individuals responsible and stop the illegal activity.

3. Federal law provides severe civil and criminal penalties for the unauthorized reproduction, distribution, or exhibition of copyrighted materials. Criminal copyright infringement is investigated by the FBI. The civil penalties for copyright infringement not registered with the Library of Congress include actual losses sustained by the copyright owner as the result of the infringement. When it comes to a registered copyright filed with the Library of Congress, the copyright owner can also obtain triple damages above and beyond actual damages, together with attorney fees in a copyright infringement case. The possible criminal penalty for copyright infringement is up to five years in prison and up to a $250,000 monetary fine. Additional details can be found at DMCA

**4.0 Methodist University Property**

The Internet and electronic communication systems, software and hardware are the property of Methodist University. All documents composed, messages and attachments sent, received, or stored on the Internet and communications storage systems are and remain the property of Methodist University. Users may not remove from the premises any hardware, software, sensitive files, or data without prior authorization by the President or appropriate Vice President.

**5.0 Network Security/Unauthorized Computer Equipment**

It is against University policy for anyone to connect any device to the campus network that will allow additional equipment to be connected. Such devices include, but are not limited to; Wireless Access Points, bridges, routers, switches, hardware and software servers, transceivers, converters, hubs, printers, concentrators, etc.. Users are not authorized to attach anything to the Methodist University Network that isn't approved by the Computing Services Department. Any Unauthorized attempts to access campus resources or any disruptive behavior on the campus network or systems will be considered a violation of University policy.

**6.0 Shared Resources**

1. Faculty, staff, and students shall use Methodist University computing resources for Academic and University-related work consistent with the stated mission of the University. While incidental and occasional personal use that does not interfere with work performance or compromise the university network is allowed, Methodist University retains sole and absolute discretion to determine when any use interferes with the University's educational and related missions and/or otherwise violates this policy and to take appropriate action. No one shall use University resources for personal financial gain or any activity that would jeopardize the tax-exempt status of the University. The University will not be responsible for unauthorized debts or obligations incurred by users.

2. Although there is no set bandwidth or other limits applicable to all users, Methodist University requires users of these resources to limit or refrain from specific uses in accordance with the principles stated elsewhere in this policy. The University makes internet resources available to students, faculty and staff to further the University's educational, research, medical, service and University-related activities and missions. Recognizing that the Internet is also an integral part of socialization and leisure among students living on campus, the network is available to students for purposes of non-academic communications and entertainment to the extent that such use does not compromise the network or the amount of bandwidth available for academic-related uses.

**7.0 Data Security**

1. All users who are authorized to use the Methodist University Student Information System (SIS) (Jenzabar) or any other secured non-public resources are required to exercise diligence and discretion to ensure that confidential information contained within the Methodist University systems are protected against

unauthorized disclosure. This means safeguarding passwords, as well as informing the Computer Services Staff immediately when a user suspects that security has been compromised.

2. Each user is required to have a unique account login and password that is not, for any reason, to be shared with another individual regardless of his or her stature at the University. Users are also required to lock or log off of any computer when they are not physically present and in front of the keyboard of the computer/laptop. Each user must confine the use of the information contained in the Methodist University SIS or other secured resources to official needs. Individual users must not allow unauthorized parties to load software on their systems, and not download information onto removable media of any kind without proper authorization.

## 8.0 Right to Monitor, Privacy, and Network Monitoring

1. Methodist University owns the rights to all data and files on any computer, network server, network system, or other information system used at the university. The University also reserves the right to monitor any and all aspects of its computer and network resources including, but not limited to, sites, instant messaging systems, chat groups, or news groups visited by users, material downloaded or uploaded by users, and e-mail sent or received by users.

2. Notwithstanding anything else herein to the contrary, no user should have any expectation of privacy in any message, file, image, or data sent, retrieved, or received while using Methodist University's computer technology. Users must be aware that the electronic mail messages sent and received using university equipment, provided Internet access, including web-based messaging systems used with such systems or access, are not private and are subject to viewing, downloading, inspection, release, and archiving at all times. Monitoring may occur at any time, without notice, and without the user's permission.

3. The University, in its sole and absolute discretion, may determine that certain broad concerns outweigh the value of a user's alleged expectation of privacy and warrant University access to relevant systems without the prior notification of the user. No user may access another employee's computer, computer files, or electronic mail messages without prior authorization from either the employee, University President, or Vice-President(s) of that individual's department.

4. Although a respect for privacy is fundamental to the University's policies, it is important to understand that almost any information can, in principle, be read or copied; that some user information is maintained in system logs as a part of responsible computer system maintenance; that the University must reserve the right to examine computer files; and that, in rare circumstances, the University may be compelled by law or policy to examine even personal and confidential information maintained on University computing facilities.

5. Any authorized user who abuses the University provided access to e-mail, the Internet, or other electronic communications or networks, including social media, may be denied future access, and, if appropriate, be subject to disciplinary action up to and including termination, within the limitations of any applicable federal, state or local laws

## 9.0 Mobile Devices

1. In the case of privately-owned mobile devices including laptops, smartphones and tablets, users must remove any personal or institutional data before disposal or recycling. Authorized users of the university who utilize a laptop or mobile device (e.g. portable hard drive, USB flash drive, smartphone, tablet) are responsible for the security of university data stored, process or transmitted to or from that mobile device. This includes physical theft, loss, and electronic invasion whether it is unintentional or intentional. It is the responsibility of the user to protect that data.

2. The use of unprotected Mobile Devices to access or store University information of any kind is prohibited regardless of whether the equipment is owned or managed by the university. At a minimum, both the device and any sensitive data should be password protected. Never leave a University or personally-owned mobile device unattended. If a university-owned mobile device is lost or stolen, immediately contact the Police and Public Safety Office at 910-630-7149/4577, and the Computer Services Department at 910-630-7020.

## 10.0 Prohibited Activities

Certain activities are prohibited when using the Internet or electronic communications. These include but are not limited to:

- Downloading or transmitting fraudulent, threatening, obscene, intimidating, defamatory, harassing, cyberbullying, discriminatory, or otherwise unlawful messages or images;
- Installing or downloading computer software, programs, or executable files contrary to policy;
- Uploading or downloading copyrighted materials or proprietary firm information contrary to policy;
- Uploading or downloading access-restricted university information contrary to policy;
- Sending e-mail using another's identity, an assumed name, or anonymously;
- Uploading or downloading applications such as peer-to-peer file-swapping tools and unauthorized enhancements and plug-ins.

## 11.0 Pornography and Sexually Explicit Content

1. Unless such use is for a scholarly or medical purpose or pursuant to a formal University investigation, users may not utilize Methodist University technology resources or privately owned devices that are attached to the University's network to store, display, or disseminate pornographic or other sexually explicit content.

2. Child pornography is illegal. The use of Methodist University technology resources or privately owned devices that are attached to the University's network to store, display, or disseminate pornographic or other sexually explicit content is strictly prohibited. Any such use must be and will be reported immediately to the Methodist University Police and Public Safety, local authorities, and Computer Services Department.

## 12.0 Violations and Enforcement Procedures

1. All users shall abide by all applicable state and federal law pertaining to communications. Computer Services is authorized by the University to investigate policy violations and apply temporary reduction or elimination of access privileges while the matter is under review.

2. All violations of the above policies will be investigated by University authorities and/or law enforcement agencies as needed. At such time that a violation is discovered, the Computer Services Staff will take the appropriate action to immediately curtail the activity. This includes, but is not limited to, the immediate revocation of all rights on computer systems at Methodist University. In carrying out an investigation pertaining to the violation of any of the above policies, or the violation of any University policy, it may become necessary for University authorities to examine files, accounting information, printouts, tapes, or any other materials. For reasons of potential liability, the University reserves the right to monitor all communications whether it be email, files on servers, or computer/laptops hard drives. Users should be aware of this fact and the fact that any computer correspondence can be used against them in disciplinary actions within the University disciplinary system, as well as used as evidence in a court of law.

Depending on the role of the individual, authorization by the appropriate University Office will be sought before any access to electronic data occurs. In the case of students, the Vice President for Student Affairs and

Dean of Students would be consulted. For faculty, permission would be obtained from the Executive VP and Academic Dean and for staff, the appropriate University Vice President would be notified.

Unless prohibited by law, a University user accused of a violation will be notified of the charge and will have an opportunity to respond to the University disciplinary body appropriate to the violator's status, before a final determination of any penalty. In addition to discipline by Methodist University, users may be subject to criminal prosecution, civil liability, or both, for unlawful use of any University systems.

Penalties for the violations of the above provisions may include, but are not limited to, expulsion, suspension, and discharge from employment, and possible prosecution by state and federal authorities. Use of the Methodist University computer system(s) signifies acceptance of the Methodist University Computer Use Policy.