MISSISSIPPI VALLEY STATE UNIVERSITY

SOCIAL MEDIA POLICY

Personal use of blogs and other social media sites such as Twitter, Facebook, and YouTube should not be utilized during work time. Employees should use their best judgment when expressing views in a blog or online sites to ensure that personal views are not construed as representing the views of the University. Information posted on online sites must not contain confidential, copyrighted, or trademarked information or marks of the University without specific written consent or license.

Internet, E-Mail, and Social Media Use

This policy outlines expectations for all employees of Mississippi Valley State University in regard to the use of Internet, e-mail, and related technologies. The policy will be administered in compliance with applicable federal, state, and local laws.

The University may provide employees with Internet/e-mail access as a tool to utilize in the pursuit of job-related activities. Although this access is intended for business purposes, personal use is acceptable as long as it is limited, occasional, and incidental. It must also be done in a professional manner that does not interfere with business use and/or job performance, including productivity. Employees are expected to demonstrate a sense of responsibility and may not abuse this privilege.

This policy includes the use and/or access of all current technological means of communication, including instant messaging, and any other means that are forthcoming.

All Internet data that is composed, transmitted, or received via MVSU computer systems is considered to be part of the University's official records. Therefore, the data is subject to disclosure to law enforcement representatives and other third parties.

The University reserves the right to monitor, retrieve, read, and record any and all uses made through an access, whether Internet or e-mail, without notice to the user. Both access and any associated communications are considered to be the business property of the organization. Employees should not expect that their messages received at work or transmitted from work are private. Employees should not expect that any messages are private or confidential, regardless of whether the e-mail is sent to or received from a work or personal e-mail address. Even when a message is erased, it can be retrieved and read.

It is a violation of this policy for any employee or other individuals to intentionally damage e-mails. Damage is defined as any impairment to the integrity or availability of data, a program, a system, or information. Damage includes intentionally accessing a computer without authorization and, as a result, causing damage. It also includes transmitting a program, information, code, or command, and as a result of such conduct, intentionally causing damage without authorization, to a computer. Legal action may be taken for such occurrences during employment or upon or after termination.

All Internet/e-mail users are expected to abide by generally accepted rules of etiquette. Employees should ensure that the information contained in these messages and other transmissions is accurate, appropriate, ethical, respectful, and lawful.

The organization does not allow data that is composed, transmitted, accessed, or received via the Internet to contain content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating, or disruptive to any employee or other person. Examples of unacceptable content include sexual comments or images, racial slurs, gender-specific comments, or other comments or images that could reasonably offend someone on the basis of race, sex, color, religion, age, national origin, disability, veteran's status, genetic information, or any other basis prohibited by federal, state, or local law.

The University does not allow the unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material on the Internet. As a general rule, if an employee did not create the material, does not own rights to it, or has not received authorization for its use, the employee may not put the material on the Internet. Each employee is also responsible for ensuring that any person sending materials of this nature over the Internet has the appropriate distribution rights.

If any user receives or obtains information to which he/she is not entitled, the employee should immediately report this situation to the Information Technology Department.

Employees should use professional judgment and be prudent in their actions, recognizing that their online presence can reflect on the University. Examples of situations that employees should self-monitor and avoid include speaking in a manner that appears to represent the organization without prior authorization; using logos, trademarks, or other intellectual property of the organization on the author’s web page without prior approval; providing official messages from the organization without a disclaimer that the views expressed are personal and not those of the organization; creating a link from a blog, website, or other social networking site to the University’s website without identifying himself/herself as an employee of the organization; being involved in harassment, discrimination, or other behaviors barred by law or University policy; and disclosing any confidential or proprietary information of the organization.

Supervision will not make work-related recommendations or references of employees on social media sites.

This policy will not be construed or applied in a way that interferes with employees' rights under any applicable state or federal labor law.

All employees are responsible for reporting any incidents that appear to be in violation of this policy to the Information Technology or the Office of Human Resources, as appropriate, for investigation.

Employees are expected to cooperate in any investigation conducted by the University.

Violations of this policy may result in disciplinary action up to and including termination of employment.