Electronic Use

Jefferson College encourages the use of electronic services for effective communication, and as an effective resource for staff and students. All personnel should remember that electronic services are assets provided through taxes and other funding. The College is the custodian of that property and must ensure use of electronic resources serves to facilitate and support the College’s educational goals.

Electronic Communications

This policy cannot cover every possible situation. Rather, it expresses the College’s philosophy and sets forth general principles that personnel should apply when using electronic services. This category includes, but is not limited to, the following College-owned or College-accessed electronic resources: computers, the network -both wired and wireless, electronic mail, electronic records, telephones, cell phones, voice mail, pagers, fax machines, printers, document scanners, copiers, hand held devices, internet resources, and wire services. This policy also covers applicable copyright laws and software license agreements.

No Expectation of Privacy

It should be emphasized that College personnel should have no expectation of privacy when using or communicating through the College’s electronic services. The Colleges reserves the right at any time and without prior notice to monitor and review employee use of College computers, networks, technology, e-mail service, internet access, and other electronic resources, to ensure that such use is made in accordance with this policy. Additionally, as required by federal law, the College does monitor general use with electronic filtering devices. In cases where inappropriate use is suspected, the College will, and does, monitor and review employee use of the College’s computers, networks, technology, e-mail service, internet access, and other electronic resources to ensure that such use is made in accordance with this policy. Such monitoring may include a review of any College computer, computer hard drive, and/or any file located or stored on a College computer, computer hard drive, or system; a review of information accessed, viewed, transmitted, or stored on the system; and a review of any and all internet sites, web sites, and areas of the internet which have been visited or accessed by a College computer or from the College system. Accordingly, e-mail and e-mail files, like all data stored or transmitted on College computers, are subject to review by College personnel at any time. Thus employees have no right to privacy with regard to any such data.

Prohibited Conduct

The following provisions apply to employee use of electronic services:

Vandalism of the network is defined as any malicious attempt to alter, harm, or destroy equipment or data of another user, the College information service or the other networks that are connected to the internet. This includes, but is not limited to the uploading or the creation of computer viruses, the alteration of data, or the unauthorized access to or theft of restricted information. Any vandalism of the College computer equipment or electronic resources will result in the immediate loss of computer service, disciplinary action and, if appropriate, referral to law enforcement officials.
One fundamental need for acceptable employee use of the College’s electronic resources is respect for, and protection of, password/account code security, as well as restricted database files, and information banks. Personal passwords/account codes may be created to protect employees utilizing electronic resources to complete work or to conduct research. These passwords/account codes shall not be shared with others; nor shall employees use another person’s password except in the authorized maintenance and monitoring of the network. The maintenance of strict control of passwords/account codes protects employees from wrongful accusation of misuse of electronic resources or violation of the district policy, state or federal law. Employees will be held accountable for the consequences of intentional or negligent disclosure of this information.

The account codes/passwords provided to each user are intended for the exclusive use of that person. Any problems which arise from the users sharing his/her account code/password, are the responsibility of the account holder. Any misuse may result in the suspension or revocation of account privileges, as well as other discipline up to and including termination. The use of an account by someone other than the registered holder will be grounds for loss of access privileges to the information system, as well as other discipline up to and including termination.

Objectionable or Harmful Material Prohibited

To the maximum extent permitted by law, employees are prohibited from obtaining, downloading, viewing or otherwise gaining access to materials which may be deemed unlawful, harmful, abusive, obscene, pornographic, descriptive of destructive devices, or otherwise objectionable or prohibited under applicable legal definitions. An exception to this prohibition exists for a College employee engaging in or assisting in faculty research on a topic related to his/her discipline. “Hacking” and Vandalism of the Network or Technology System Prohibited

Employees who engage in investigatory activities commonly described as “hacking” are subject to loss of privileges and to discipline. Hacking may be described as the unauthorized review, duplication, dissemination, removal, damage, or alteration of files, passwords, computer systems, or programs, or other property of the College, a business, or any other governmental agency obtained through unauthorized means, such as gaining access into restricted information on systems or network files in violation of password/account code restrictions.

Security/Safeguarding Accounts and Passwords

The College recognizes that security on its electronic network is an extremely high priority. Security poses challenges for collective and individual users. Any intrusion into secure areas by those not permitted such privileges creates a risk for all users of the information system.
Advertising or Soliciting Prohibited

Employees are prohibited from advertising or soliciting on the College’s computer equipment and electronic resources. This includes commercial advertisement for products or services (such as Amway, Avon or Tupperware) as well as fundraising, non-profit, or charitable solicitation. Any exceptions must be approved in advance by the appropriate Vice President. Non-work related messages clutter the e-mail system, absorb system resources, and are unwelcome to many recipients. Employees are similarly prohibited from sending e-mail on such topics to the district e-mail system from home or other outside computers.

Inappropriate and/or Frequent Personal Use

Because the College is a public governmental body, employee computer use may be subject to Missouri’s Sunshine Law, meaning that employees may be required to turn over their personal e-mail and other computer records to the public on request. As a result, this policy allows occasional, incidental personal use of the College’s electronic services but sets restrictions on such use.

College resources are to be used primarily for work-related purposes and any personal use must be on the user’s own time. Incidental, personal use must not violate any of the rules contained in this policy or any other College’s employment policy, and must not damage the College’s hardware, software or network systems. All extenuating circumstances should be approved by the employee’s supervisor and authorized by the Technology Department.

Examples of Inappropriate Behavior

Behaviors which violate this policy, and will result in loss of access and/or discipline shall include, but are not limited to, any of the following: damage to or theft of system hardware or software; alteration of system software; placement of unlawful information, computer viruses or harmful programs on or through the computer system; gaining access to restricted information on system or network files in violation of password/account code restrictions; any violation of students’ rights to privacy; violation of other users’ right to privacy; using another person’s name to send or receive messages on the network; sending or receiving personal messages including jokes, etc. on College time; transmitting information seeking employment outside of the College; and use of the network for personal gain, gambling, cyber-bullying, personal instant messaging, commercial purposes, or to engage in political activity. Commercial or non-work-related chain letters, “chat rooms” are prohibited, with the exception of those bulletin boards or “chat” groups that are for specific work related communication. Downloading and installing non-College approved applications, shareware, freeware and games is prohibited as this consumes College resources and often results in costly side effects. It is also prohibited to post or participate in online forums, blogs, and/or social networking sites when such posting or participation will result in a violation of Missouri or federal laws, contains obscene, threatening, or libelous material, or violates another person’s right to privacy. Other examples of inappropriate behavior are addressed below.
Violation of Copyrights and Software Licenses

Absent an agreement between the College and an employee, an employee may not claim personal copyright over files, data or materials, developed in the scope of their employment. This procedure prohibits illegal publication or copying of copyrighted material, or other use of copyrighted materials without the permission of the copyright holder. This policy also prohibits illegal copying of software or other use of software. The connections represented by internet access and electronic resources allow users to access a wide variety of media. Even though it is possible to download most of these materials, employees shall not create or maintain archived copies of these materials unless the source indicates that the materials are in the public domain. Employees will be held personally liable for any of their own actions that violate copyright laws or software agreements.

Other Disciplinary Rules and Employment Policies Apply

As noted above, the use of the district computer technology and electronic resources is a privilege, not a right. The proper exercise of this privilege requires employees to maintain high levels of personal responsibility. All existing employment policies and rules of employee conduct found in the College’s policies, employee handbooks, and similar documents apply with equal force to employees in their use of the College’s computer technology and other electronic resources, including their use of the e-mail system and internet access.

Non-exempt Employee Electronic Communications

As with other types of unauthorized work, all time spent by nonexempt employees utilizing electronic communications for work purposes will be considered hours worked, is compensable and count toward overtime eligibility as required by law. Therefore, in order to avoid incurring unnecessary expenses, electronic communications should not be used outside of regularly scheduled work hours unless required by management. This includes all types of work-related communication.

Consequences for Violation of Policy

It is also the responsibility of College personnel to follow all College policies and procedures as well as state and federal statutes and laws. The consequences for violating the district’s EUP include, but are not limited to, one or more of the following:

- Suspension of computer access
- Revocation of computer access
- Employee disciplinary action up to and including dismissal
- Referral to law enforcement agency
- Excessive personal use can interfere with performance of job duties and is a waste or misuse of College resources. Employees who abuse the privilege of College facilitated access to electronic services are subject to corrective action and risk having the privilege removed for themselves and possibly other employees.

Refer to Board Procedure II-001.3.
Official E-mail Communication

Upon being hired, the Office of Human Resources will initiate the establishment of a college email address and services for employees. To insure effective and timely communications of important information from the College, all employees must check the college-provided email regularly.

Refer to Administrative Procedure II-006.

Progressive Disciplinary Action

The College adheres to the principle of progressive discipline with respect to its employees. This means that degrees of discipline are generally progressive and are used to ensure that the employee has the opportunity to correct his or her performance. There is no set standard of how many oral warnings must be given prior to a written warning or how many written warnings must precede suspension or how many suspensions must precede termination. Factors to be considered are:

• how many different offenses are involved
• the seriousness of the offense
• the time interval and employee response to prior disciplinary action(s)
• previous work history of the employee

In General

Several oral warnings should, at the next infraction, be followed by a written warning, followed by suspension, followed at the next infraction by discharge. This is especially true in those cases where the time interval between offenses is short and the employee demonstrates a poor desire to improve his/her performance. Supervisors should document all oral and written warnings to demonstrate that an opportunity for correction of the behavior was accorded to the employee.

Exception

For serious offenses, such as fighting, theft, insubordination, threats of violence, the sale or possession of drugs, or abuse of alcohol on College property, termination may be the first and only disciplinary step taken. Insubordination is defined as the refusal or failure to obey a lawful directive of a supervisor or superior. Any step or steps of the disciplinary process may be skipped at the discretion of the College officials after investigation and analysis of the total situation, past practice, and circumstances.

When questions arise as to how to discipline an employee, supervisors are encouraged to consult with the Director of Human Resources. Where there is a discharge recommendation, the Director of Human Resources shall provide leadership for the process in order to assure that discipline is imposed and due process procedures followed in accordance with personnel policies.

In the interests of both the employee and the College, any investigation of potential disciplinary situations should be concluded expeditiously.

Refer to Board Procedure II-001.4.