Acceptable Use of College Technology Resources

What is "acceptable use"? Why is it important? Why now?

This document is a reminder to the campus about the policies and procedures that describe the acceptable use of technology resources. The policy itself and the procedures that support the policy have not changed but technical environment has changed. The campus should be aware of the possible results of the technology changes.

The employee handbook contains a section called "Use of College Information and Time" and the first item in the section addresses technology resources. The handbook outlines acceptable use of these resources which include, among other items, phones, printers, copiers, computers, software, and internet access. The essence of the policy is as follows, although the handbook is the authoritative source if there are inconsistencies between it and this description.

Technology resources are here for college business. The college has established and enforces policies that protect the resources and the college's ability to use them for teaching, learning, operations, residential life and other functions.

Employees may use technology resources for personal use within reason. If an employee's personal use of the resources is excessive the college may ask for reimbursement from the employee. Employees have been responsible; there may have never been a request for reimbursement.

Employee use may not break the law, for example, illegal downloading. Nor may employees use the equipment to violate any other aspect of the code of conduct, for example, for harassment of any type. If there is an incident, the handbook outlines the procedure that is used to find a resolution to the issue.

Information Technology's primary responsibility is to keep the resources secure and capable of meeting the business needs of the college. Beyond that, the department does not examine logs, which contain data describing activity on computers or accounts, or files of employees unless there is an indication that a particular computer, computers, account, or accounts may have been compromised by a malicious attack or misused in some other way. In that case, IT must thoroughly understand the causes and risks of such use and respond as necessary to prevent any disruption in network availability, loss of information, or college liability. Examples of malicious attacks include activities like spreading a computer virus, using malware to corrupt data, or using phishing schemes to steal passwords.

Employees should understand that as the sophistication of the attackers has increased so has the power of the tools that IT uses to protect the college and its employees from those attacks. One of the consequences of using more powerful tools is more knowledge about the use of the computer or account in question, for example, web sites visited. From time to time, the process of removing a virus or discovering malware will reveal a potential or actual violation of the policy on acceptable use of technical resources.

The vast majority of these violations are unintentional and/or accidental. In those cases, we ask the IT staff to do some education about malicious web sites and best practices for web surfing, downloading and cyber safety in general. The college has had a few, fortunately very few, incidents where the violation was serious and warranted immediate intervention.

Employees should be aware that in certain situations their logs and files could be examined by IT staff and others. The new tools the department uses to protect the resources will probably increase the number of times staff will examine logs and files. If an examination indicates that there may be a violation of the policy, the resulting inquiry could lead to a variety of consequences. IT does not routinely examine files or logs, and has no time or inclination to do so, but the department must meet its obligation to protect the network, all users and the college. Please read the handbook for all the details.

Certainly, college systems are attacked even when the resources are used for business purposes but personal use accounts for the bulk of incidents. Employees may reduce the risk of malicious attacks and reduce any related privacy concerns by minimizing their personal use of the resources.

Additional details regarding acceptable use of college technology resources can be found in the following documents on the portal.

- Acceptable Use Policy
- Employee Handbook (Technology Resources)
- Student Code of Conduct and College Policies (Electronic Information Policy)