

**Responding to Internet and Computer Misuse
An Overview for MnSCU HR Professionals**

**Rebecca Wodziak, Principal Labor Relations Representative
MnSCU Office of the Chancellor**

I. Introduction.

The following is a brief summary of the employer's approach to employee's misuse and abuse of the employer's computer resources. This is not intended to be a complete guide to handling computer misconduct by employees. All cases of alleged computer misconduct should be fully investigated; any decisions regarding employee discipline must be based on the specific details of the misconduct and the specific circumstances surrounding the employee's actions.

Questions about investigations or possible discipline should be directed to the staff at MnSCU Labor Relations. Questions regarding alleged illegal activity should be directed to MnSCU's Office of General Counsel and/or the Attorney General's Office, as well as brought to the attention of MnSCU Labor Relations.

II. General Principals.

- A. Computer misconduct is not "special" or unique. Misuse of computer resources is simply ordinary misconduct; it should be viewed in the same light as the misuse of any kind of employer's property such as telephones, fax machines, cars, laboratory equipment etc.
- B. Computers and the technology that accompanies them (e-mail, web sites, the internet, etc.) are all considered the employer's property. Employee's do not have an unrestricted right to privacy on their workplace computers.
- C. There are many kinds of misconduct that can be committed with computers. This is not just about surfing pornographic web sites.
- D. College or University HR professionals should be prepared to respond to allegations of illegal computer activity. Know whom to call if illegal activities are alleged.

III. Tips for Avoiding Problems.

- A. Have a clear policy. Employees cannot be held responsible for rules that we have not communicated to them.
- B. Communicate the policy to all administrative and managerial personnel as well as faculty and staff.

- C. Be prepared! Have a “general plan” in place for investigating alleged misconduct. Do not wait for a crisis to develop to think about the basics of conducting investigations. Try and identify, in advance, how your institution will respond to the following kinds of issues:
- i. To whom are allegations of computer misconduct reported?
 - ii. Who will investigate?
 - iii. How will the investigator coordinate their activities with the IT staff, the General Counsel’s Office and, if necessary, law enforcement agencies?
 - iv. Ensure that the investigator knows:
 - when to contact law enforcement agencies;
 - how to maintain data privacy;
 - what limitations exist on their ability to search and or seize employee’s computer records?
 - v. How does the investigator determine when special security measures must be taken, to maintain the integrity of the employer’s computer system or to preserve evidence of employee misconduct?
- D. Get advice and assistance when problems are discovered.
- E. Be sure to obtain legal advice before attempting to search personal property, including files that are marked as “personal” or personal e-mail accounts housed on MnSCU computers or any unopened e-mail.

IV. Understanding the State of Minnesota’s Policy on Appropriate use of Electronic Communication Technology.

- A. This (DOER) policy currently applies to all of MnSCU and its employees. A specific policy, unique to MnSCU is under development at this time.
- B. DOER policy defines acceptable use.
- C. DOER policy permits some personal use “...provided this use, including the value of the time spent, results in no incremental cost to the state or results in an incremental cost that is so small as to make accounting for it unreasonable or administratively impractical.” (MS. 43A.38, Subd. 4.)
- D. All employee use of the employer’s communication technology (personal and professional) “... must be able to withstand public scrutiny without embarrassment to the agency (MnSCU) or the State of Minnesota.”
- E. DOER policy lists examples of inappropriate use. These include but are not limited to: illegal activities; gambling; sales or other activities for personal gain or profit; harassment or disparagement of others; fundraising; promotion of political activities; downloading or installing software; receipt or transmission or storage

of materials that could reasonably be regarded as violent, harassing or discriminatory, obscene, sexually explicit or pornographic; unauthorized access to non-public data, union organizing or campaigning.

- F. Colleges and universities are free (even encouraged) to develop policies that identify unacceptable use and specify protocols for handling such issues. Suggestions for items that are considered unacceptable could include: spamming, chain letters, accessing pornographic or other sexually explicit sites for personal amusement, use of the computer for personal gain, political activity, copyright infringement (remember NAPSTER?)
- G. Employees should be clearly advised that their computer use may be monitored by the employer. College or University policies should specify that employee's privacy rights are limited and that their computer use can be monitored. (Note that in the DOER Policy, the section on monitoring states: "...Employees should not expect that any facsimile, voicemail, or e-mail message either sent or received or any Internet activities will remain private.")

V. Considerations Unique to MnSCU

- A. Academic freedom.
- B. Copyright infringement.
- C. Faculty members desire to protect their intellectual property.
- D. Student data.
- E. Student privacy (expectations of privacy are higher than employees.)
- F. Maintaining an atmosphere of free intellectual inquiry while protecting the employer from liability and allegations of impropriety.