Federal Employee Computer Use

Here we are in 2007. Most Federal employees have had a computer on the desk for the last 20 years. A usable (for non-IT experts) internet has been widely available for the last 10 years. Email has effectively wiped out all but the most official or legal intra-agency document in most organizations. Many agencies have also had authorized use policies in effect for the last ten years. Everybody knows the rules so no problems, huh? Apparently not. In asking around and reading cases. It appears computer misuse or at least agency concerns about it are evolving as fast as the medium.

Let’s take a look at what agencies allow and don’t, what’s new and what Federal managers and employees should worry about.

The General Environment

Getting legal, the computer on the desk belongs to Uncle Sam. Agencies get to decide what it can and can’t be used for. It also appears that the “reasonable expectation of privacy” concept that has been accepted in the past as preventing searches of personally owned purses and briefcases or government owned desk drawers and lockers won’t help with regard to the computer. Since 9/11, I’m not sure those arguments will work as well either but the jury (oops! Arbitrator or MSPB) is still out on that.

The Federal Labor Relations Authority said no to union proposals on limiting management’s control based on privacy arguments. The FLRA appears to rely on an “internal security procedures” –based argument (take a look at 60 FLRA No. 29 8/10/04) in its decision. On a side note the Authority in the above case refers to another case in which a notice appears when an employee signs on. My take is that they are giving agencies advice (Got It?). The Merit Systems Protection Board has also taken a dim view of inappropriate use in a number of cases. Justice also has computer crime and fraud laws employees should pay attention to that address criminal misuse.

What’s Generally Allowed

Obviously, any work-related use is okay within security restraints in certain agencies. I don’t know but am reasonably sure that HHS employees don’t have the same constraints in attaching documents to intra-office email as do CIA or NSA folks.

Agencies with personal use policies frequently permit, on the employee’s own time, personal use of the internet if the service is procured at a fixed rate. Most policies deal with permitted internet use in the negative (see below) because of the broad nature of what’s available online. Email use policies are generally similar to those governing personal use of the agency’s telephone. Phone use is generally limited to short duration calls that deal with personal issues. Most agencies frown on long distance calls particularly if there is a charge or calls that can be made other than during work

What’s Generally Prohibited

One agency policy I looked at was fairly typical of the rest. It precluded:

- Access, retrieval, or printing text and graphics information which exceeds the bounds of generally accepted standards of good taste and ethics.

- Engaging in any unlawful activities or any other activities which would in any way bring discredit on the Department.
- Engaging in personal commercial activities on the Internet, including offering services or merchandise for sale or ordering services or merchandise from on-line vendors.
- Engaging in any activity which would compromise the security of any Government host computer. Host log-in passwords will not be disclosed or shared with other users.
- Engaging in any fund raising activity, endorsing any product or services, participating in any lobbying activity, or engaging in any active political activity.

This policy had an interesting last sentence, "The prohibition against engaging in political activity does not apply to Presidential appointees who have received Senate confirmation." I wonder if there are any limits on that. There were not any in the policy statement.

A number of agencies get very specific, making it clear that "sites that offer sexual material or defame race, gender, religion, or other protected classes" are off-limits. Many forbid the downloading of any software without specific, advance and written permission from the Chief Information Officer. If yours doesn't, it probably should.

What's New

Most office computers have the capability to view pictures or video. These features are frequently bundled with office suite software such as MS Office and the like. These suites also feature the ability to password protect (I couldn't bring myself to use the word encrypt) files or programs. While these features can enhance productivity, they may also present opportunities for mischief.

The features mentioned also allow the communication and viewing of animated graphic files, video clips, games, movies, photo albums, streaming media, on-line music, news and sports events, chain letters, and jokes. Companies like Vonage offer computer-driven internet phone service at very low cost. My new Palm Treo accepts downloads from my computer including my address book and data files and will run an MSPower Point presentation.

This all means it's getting easier to share information of all kinds and harder to monitor use and preserve the security of Agency information.

So What Should a Manager Worry About

Computer use and misuse has become the interest of virtually everyone in the workplace. Both managers and employees should be concerned. Agency IGs sweat bullets as investigation into computer abuse gets more complicated. If I were a Federal supervisor, I would make sure employees are aware of the agency policy. Make copies and get them to sign for them. Real paper and real signatures are better than virtual ones.

Advise employees to take care with what is sent and who it's sent to. Let them know that wasting work time in news groups, bulletin boards and chat rooms that aren't work related and useful is unacceptable. If employees can encrypt files or set a password, direct them to provide you a paper copy of the password and information that will allow you to access any file even if it is encrypted. Forbid downloading documents and executable files attached to e-mail from unknown outsiders. Make sure each employee has contact information for IT or whoever monitors your systems if they suspect a problem. Stress that smart computer use is also in their best interest. Strongly encourage or order the backup of any file on their hard drive that's not duplicated on the server.