

## **Department of Homeland Security** **Policy on Personal Use of Government Office Equipment**

**General.** DHS employees may use Government office equipment for authorized purposes only. As set forth below, limited personal use of the government office equipment by employees during non-work time is considered to be an "authorized use" of Government property, when such use:

1. involves minimal additional expense to the government,
2. is performed on the employee's non-work time,
3. does not reduce productivity or interfere with the mission or operations of DHS organizational elements, and
4. does not violate the Standards of Ethical Conduct for Employees of the Executive Branch (5 CFR Part 2635).

### **Authorizations**

1. Employees must be authorized to use equipment for official Government business before it is available for limited personal use.
2. DHS is not required to supply equipment if that equipment is not required to perform official Government business.
3. Managers and supervisors may further restrict personal use based on the needs of the office or problems with inappropriate use in the office.

### **Privacy Expectations**

Employees do not have any right to privacy while using any Government office equipment, including Internet or email services. Furthermore, use of Government office equipment, for whatever purpose, is not secure, private or anonymous. While using Government office equipment, employee use may be monitored or recorded. If Government office equipment or services are involved at any point in the transmission or receipt of personal information, then this policy applies and use may be monitored. For example, if a DHS employee uses a Government computer to read or respond to personal email sent to a non-Government email address (e.g., AOL, Yahoo), that use may be monitored.

### **Telephone Calls**

Business telephone calls may be monitored or recorded for legitimate business purposes such as providing training, instruction or protection against abusive calls. Personal phone conversations and business telephone calls will not be

routinely monitored. Before DHS institutes a policy to routinely monitor employees' personal or business phone conversations, employees will be notified.

### **Proper Representation**

1. DHS employees must ensure that personal use does not give the appearance of acting in an official capacity. For example, DHS employees may not post DHS information to external news groups, bulletin boards or other public forums without DHS authorization.
2. DHS employees must not give the appearance that DHS endorses or sanctions personal activities. If an employee's actions leave the impression that his/her personal activities are endorsed by DHS, the employee may be in violation of the Standards of Ethical Conduct for Executive Branch Employees.
3. DHS employees must make every effort to avoid the potential for confusion. If there is any potential for confusion, employees must provide an appropriate disclaimer, such as:

***“The content of this message is mine personally and does not reflect any position of the Government or of DHS.”***

### **Inappropriate Personal Uses**

1. Using large files. Activities might reduce the effectiveness of a DHS system if sending large files electronically. For example, sending or receiving greeting cards, video, sound, interactive games or other large file attachments may hinder the performance of an entire network. Employees should not subscribe to Internet services that automatically download information, such as sports scores, stock prices or other continuous data streams, such as music or videos.
2. Loading personal software onto a government computer or making configuration changes. For example, computer games, personal tax programs and personal schedulers may not be loaded on DHS computers.
3. Engaging in email practices that involve ongoing message receipt and transmission, referred to as “instant messaging.”
4. Making personal long distance telephone calls. There are three exceptions:
  - a. in an emergency,
  - b. brief calls within the local commuting area to locations that can only be reached during working hours (e.g., car repair shop, doctor), and
  - c. brief calls home within the local commuting area (e.g., to arrange transportation, check on a sick child).

5. Using Government equipment as a staging ground or platform to gain unauthorized access to other systems.
6. Creating, copying or transmitting chain letters or other mass mailings, regardless of the subject matter.
7. Creating, copying or transmitting any material or communication that is illegal or offensive to fellow employees or to the public, such as hate speech, material that ridicules others based on race, creed, religion, color, sex, disability, national origin or sexual orientation.
8. Viewing, downloading, storing, transmitting or copying materials that are sexually explicit or sexually oriented, related to gambling, illegal weapons, terrorist activities or any other prohibited activities.
9. Using Government office equipment for commercial purposes or in support of other “for profit” activities such as outside employment or businesses (e.g., selling real estate, preparing tax returns for a fee).
10. Engaging in any outside fund raising activity, endorsing any product or service, participating in lobbying or prohibited partisan political activity (e.g., expressing opinions about candidates, distributing campaign literature).
11. Acquiring, reproducing, transmitting, distributing or using any controlled information including computer software and data, protected by copyright, trademark, privacy laws, other proprietary data or material with other intellectual property rights beyond fair use, or export-controlled software or data.

### **Sanctions for Misuse of Government Equipment**

Unauthorized or inappropriate use of Government office equipment may result in the loss or limitation of an employee’s privilege. Employees may also face administrative action ranging from counseling to removal from the Agency, as well as any criminal penalties or financial liability, depending on the severity of the misuse.

For more information on this DHS policy please refer to DHS Interim Management Directive Number 4600 or contact the Office of the Chief Information Officer (CIO).