

1-6

USE OF STATE RESOURCES

DATE: January 31, 2003

CANCELS: Previous policy dated October 8, 1998, June 4, 1998 and June 30, 1998.

CONTACT: Marie DeLong

SCOPE: All WSHS Employees

APPROVED BY: _____ **DATE:** _____

PURPOSE

The purpose of this policy is to communicate to WSHS employees their limits and responsibility for proper use of state resources. The same limitations and responsibilities apply to all contractors who use state resources in performing services for WSHS.

Definitions

“State resources” include, but are not limited to information technology assets, computer platforms, micro- or personal computers, mini-computers, mainframes, workstations, data resources, electronic message systems, software, software licenses, facilities, vehicles, Internet connections or accounts, credit cards, supplies, volume discounts, documentation, the state mail service, copyrighted material, SCAN service, copiers, fax machines, telephones and cellular phones.

“Electronic message systems” means electronic mail (E-mail) systems which store and transmit typed communications, including the Internet; voice mail systems which store and transmit voice communications; facsimile and imaging equipment which store and transmit images; and all similar systems.

“Internet” means the connection to and use of interconnected networks in the public and private domains through the use of computer workstations that operate software to access World Wide Web, Gopher, file transfer protocol (Ftp), and other network resources.

POLICY

State Resources for WSHS Business

WSHS employees who use state-owned resources are responsible for using the resources in an ethical, legal and conservative manner. The resources detailed above are provided

APPROVED
Executive Ethics Board

Date: 1/10/03

to employees as tools to help them conduct WSHS business. They may never be used for transmission of information that promotes discrimination on the basis of race, creed, color, gender, religion, handicap, sexual preference; sexual harassment; copyright infringement; promotion of personal political beliefs; personal business or other personal interest including sexually explicit material; or any unlawful activity. In most circumstances employees are not to use state-owned equipment, services, information technology, or other resources for personal purposes. In some instances, limited use of state resources which does not result in additional costs to the state, such as local telephone calls, is permissible. Employees are trusted to exercise good judgment in both the duration and frequency of such occasions. Long distance calls for non-business reasons should not be made in a way that results in charges to WSHS, except that employees on travel status may place brief (10 minutes or less), calls to their homes or families to communicate safe arrival or changes in itinerary.

Use of Electronic Message Systems

WSHS electronic message systems are provided as productivity tools for employees to regularly conduct official business. Infrequent use of electronic mail is allowed provided that it is not used for private benefit or gain; has not been removed from the state facility or official work station, for supporting, promoting, or soliciting for an outside organization, unless authorized by the agency head or designee; for commercial use such as advertising or selling; campaign or political use or any illegal activity; to access computer networks, other data bases, electronic bulletin boards for personal use, unrelated to official business.

Electronic Message Systems Privacy and Security

Employees are expected to respect the privacy of others by not sending unwanted E-mail or voice mail messages, misrepresenting others when sending E-mail or voice mail, or tampering with others' E-mail or voice mail accounts, files or data.

Electronic message systems may not be secure. Employees should be aware of potential electronic messaging security problems before transmitting private or confidential messages. Potential problems include:

Disclosure: An unauthorized user may gain access to electronic messages. Disclosure often occurs inadvertently. Disclosure may occur when messages are: forwarded to unauthorized users; directed to the wrong recipient; or printed in a common area where others can read them. Pass code disclosure can also occur.

Message Modification: Message contents or delivery time may be altered.

Masquerading: An authorized user may appear to the system to be another user to gain access to information.

Review of Electronic Messages

WSHS does not monitor electronic messages, such as E-mail notes or voice messages, on a regular basis. The maintenance and operation of electronic message systems may result

APPROVED
Executive Ethics Board

Date: 1/10/03

in observation of random messages. Managers may access data under employees' control to conduct WSHS business or to prevent misuse. Managers may obtain the director's approval to monitor messages during the course of investigating improper or illegal activity.

Electronic Mail Messages as Public Records

The Attorney General's Office, the State Auditor's Office, the Office of Financial Management and the State Archivist have determined that certain electronic mail messages constitute public records which must be retained and preserved, and which may be disclosed to requesters. E-mail messages are stored in the network without action by the sender. If a WSHS employee transmits an E-mail message that establishes agency policy, the sender of that message must create a paper copy and retain it consistent with a records retention schedule that has been approved by the State Records Committee.

Use of Internet

Access to the Internet is provided to WSHS employees as a research and communication tool for conducting agency business. Personal use of the internet by employees is permitted if it is both brief and infrequent. WSHS provided internet access may never be used for transmission of information that promotes discrimination on the basis of race, creed, color, gender, religion, handicap, sexual preference; sexual harassment; copyright infringement; promotion of personal political beliefs; personal business or other personal interest including sexually explicit material; or any unlawful activity.

Internet Security

Employees are prohibited from downloading software from the Internet in order to prevent infection of the LAN environment.

Use of Cellular Phones

Cellular phones are provided to WSHS employees who have a demonstrated business need for them. Employees whose productivity levels are likely to rise while working in transit may request to use cellular phones. Among the employees likely to need cellular phones are executive decision makers, on-call employees and service technicians. Charges for use of cellular phones are usually much higher than conventional, wire-based telephone systems. Employees should not use cellular phones when a less costly alternative is safe, convenient, and readily available.

WSHS employees leaving state service who have had state-owned cellular equipment installed in their private vehicles may, at their option, purchase the equipment from WSHS when having the equipment removed would damage the vehicle or when the cost of removal exceeds the value of the cellular equipment. The fixed assets officer will determine the fair market value of the equipment. WSHS-owned cellular phones and

APPROVED
Executive Ethics Board

Date: 11/10/03

services are generally to be used to conduct WSHS business, except in the event of an emergency as outlined in RCW 42.18.217. Personal use of cellular telephones is not consistent with the Ethics in Public Service Act but there may be limited situations whereby officers or employees, working at a remote location, may request permission to use cellular telephones for personal use. In such instances, employees may, with the written consent of their supervisor, use state-owned cellular phones for personal use provided that they reimburse the agency for all costs including administrative costs.

Cellular Phones Security

Cellular transmissions are not secure. Employees should exercise discretion in relaying confidential information

Use of Toll Free Phone Lines

Toll free lines are provided by WSHS for calls from out of the local calling area by visitors and vendors. Employees are not to release the toll free telephone number for purposes of receiving calls of a personal nature. Monthly reports reflecting incoming calls on the toll free lines will be monitored.

Use of SCAN Lines

SCAN (Statewide Controlled Area Network) is a dedicated telephone network managed by the State to provide low cost long distance services to public entities. All business related long distance calls should be placed on SCAN. SCAN Detail Billing Reports will be distributed monthly to supervisors and to each employee for certification that all calls placed using the SCAN authorization number were made for WSHS business only.

To place SCAN calls:

- Depress appropriate key on telephone set to place a SCAN call.
- Dial 8, wait for tone.
- Dial 6-digit authorization number, wait for tone.
- Dial the area code and telephone number.

Note: Allow several seconds to elapse in between SCAN calls to ensure that the previous call has been disconnected.

Use of WSHS Phone Lines for Placing a Personal Long Distance Call

Employees may make an occasional personal long distance telephone call that is billed to a third party (collect, personal credit card or carrier's toll free access number or personal calling call).

APPROVED
Executive Ethics Board

Date: 1/10/03

- From a line that places local calls, dial your personal long distance company's carrier access code or toll free access number (1-800... or 1-888...) or dial 0 + area code and number of the person you are calling.

Use of WSHS Van

OFM regulation 4.2.5.2.2 prohibits travel in a state owned motor vehicle between duty station (your official work station) and residence with some exceptions relating to safety, health and economic advantage to the state. Prior approval by department head is required. Usage by department and division heads require approval by the director.

APPROVED
Executive Ethics Board
Date: 1/10/03