

Department Computer Use

352.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the proper use of Department information technology resources, including computers, electronic devices, hardware, software, and systems.

352.1.1 PRIVACY POLICY

Any Member utilizing any computer, electronic storage device, or media, Internet service, phone service, information conduit, system, or other wireless service provided by or funded by the Department expressly acknowledges and agrees that the use of such service, whether for business or personal use, shall remove any expectation of privacy the Member, sender, and recipient of any communication utilizing such service might otherwise have, including as to the content of any such communication. The Department also expressly reserves the right to access and audit any and all communications, including content that is sent, received, and/or stored through the use of such service.

352.1.2 DEFINITIONS

The following definitions relate to terms used within this policy:

Computer System: All computers (on-site and portable), hardware, software, and resources owned, leased, rented, or licensed by the Orange County Sheriff-Coroner Department, which are provided for official use by agency Members. This shall include all access to, and use of, Internet Service Providers (ISP) or other service providers provided by or through the agency or agency funding.

Hardware: Includes, but is not limited to, computers, computer terminals, network equipment, modems, or any other tangible computer device generally understood to comprise hardware.

Software: Includes, but is not limited to, all computer programs and applications including "shareware". This does not include files created by the individual user.

Temporary File or Permanent File or File: Any electronic document, information or data residing or located, in whole or in part, whether temporarily or permanently, on the system, including but not limited to spreadsheets, calendar entries, appointments, tasks, notes, letters, reports, or messages.

352.2 SYSTEM INSPECTION OR REVIEW

A Member's supervisor has the express authority to inspect or review the system, any and all temporary or permanent files and related electronic systems or devices, and any contents thereof when such inspection or review is in the ordinary course of his/her supervisory duties, or based on cause.

When requested by a Member's supervisor, or during the course of regular duties requiring such information, a member(s) of the agency's information systems staff may extract, download, or otherwise obtain any and all temporary or permanent files residing or located in or on the system.

Department Computer Use

Reasons for inspection or review may include, but are not limited to system malfunctions, problems, or general system failure; a lawsuit against the agency involving the Member, or related to the Member's duties; an alleged or suspected violation of a Department policy; or a need to perform or provide a service when the Member is unavailable.

352.3 AGENCY PROPERTY

All information, data, documents, communications, and other entries initiated on, sent to or from, or accessed on any Department computer, or through the Department computer system on any other computer, whether downloaded or transferred from the original Department computer, shall remain the exclusive property of the Department and shall not be available for personal or non-Departmental use without the expressed authorization of a Member's supervisor.

352.4 UNAUTHORIZED USE OF SOFTWARE

Members shall not copy or duplicate any copyrighted or licensed software except for a single copy for backup purposes in accordance with the software company's copyright and license agreement. To reduce the risk of computer virus or malicious software infection, Members shall not install any unlicensed or unauthorized software on any Department computer. Members shall not install personal copies of any software onto any Department computer. Any files or software that a Member finds necessary to upload onto a Department computer or network shall be done so only with the approval of the Department IT specialist and only after being properly scanned for malicious attachments.

No Member shall knowingly make, acquire, or use unauthorized copies of computer software not licensed to the agency while on agency premises or on an agency computer system. Such unauthorized use of software exposes the agency and involved Members to severe civil and criminal penalties.

352.5 INTERNET USE

Internet access is primarily for County business. You may access the Internet for limited personal use only during non-working time and in strict compliance with policy. If there is any doubt about whether an activity is appropriate, consult with your Department Head or his/her designee.

The Department shall actively monitor use of the Internet, to ensure that anyone using Department access to the Internet does not engage in any unethical, illegal, or unacceptable activity. Examples of unethical, illegal, or unacceptable activities include, but are not limited to:

1. Activities outlined in the section "Prohibited Activities" within the latest Orange County's Information Technology Usage Policy.
2. Seeking to gain or gaining unauthorized access to information resources.
3. Gaining, communicating, or using passwords belonging to other users.
4. Using the Internet to access, process, distribute, transmit, or display inappropriate stored electronic media; obscene, libelous or defamatory material, or any material, the access to which might undermine the integrity of the Sheriff's Department. Certain

Orange County Sheriff-Coroner Department

Orange County SD Policy Manual

Department Computer Use

exceptions may be permitted with the approval of a supervisor as a function of an assignment.

5. Participating in "chat rooms".
6. Running any type of public or unauthorized peer-to-peer network services, such as KaZaA, Gnutella, and Napster, etc.
7. Using any type of public or authorized instant messaging, such as Windows Live Messenger, Yahoo! Messenger, Skype, etc.
8. Using the Internet web-based email or private email, such as Gmail, Hotmail, and AOL.
9. The use of "Web Radio", "Web Shots", "Weather Bug", "Napster" (or the equivalent), "Web Casts", "Web Robots" or any other real-time streaming connections which occupies continuous bandwidth (resources) in the network.
10. Downloading copyrighted media and/or unlicensed software program files.

The use of the Internet is a privilege, not a right. If a Member is found to have engaged in any unethical, illegal, unacceptable activities, or violation of this policy, such activity shall subject the user to discipline consistent with any applicable labor agreement or policy including revocation of rights to Internet access.

In order to maintain network security, all Members using County access to the Internet are expected to comply with the following:

1. All files downloaded from the Internet must be scanned with anti-virus software approved by Information Services.
2. Make sure the computer which is used for Internet access is protected by anti-virus software.
3. No computer used for Internet access can be connected to another Internet Service Provider other than what is provided by the Department.

Any Member that feels he or she can identify a security concern or feels that his or her system may be infected or intruded with a computer virus should perform no further work on the computer and immediately contact the System help desk.

The Information Service Bureau reserves the rights to block accesses which are determined to pose security threats or excessive loads to the information and network infrastructure.

352.6 PROTECTION OF AGENCY SYSTEMS AND FILES

All Members have a duty to protect the system and related systems and devices from physical and environmental damage and are responsible for the correct use, operation, care, and maintenance of the system.

It is expressly prohibited for a Member to allow an unauthorized user to access the system at any time or for any reason.

Orange County Sheriff-Coroner Department

Orange County SD Policy Manual

Department Computer Use

352.6.1 STORAGE

Network drive space is a resource provided for the purpose of storing work-related materials and files. All Members are responsible for managing this space, which includes deleting nonessential or obsolete files to keep space utilization at a minimum. Personal media files such as music files, personal images, or personal video clips are not to be stored on network drives. The Department allots a specific amount of network drive space to meet the needs of individuals and Departments. Information Systems is responsible for monitoring network drive space and notifying individuals and Departments when they exceed the allotted space. Individuals and Departments may request a quota increase. Upon receipt of a request, the drive space shall be reviewed for compliance with the data storage policy. Additional space may be allocated based upon need and availability of resources.

352.6.2 NETWORK DRIVES

The following is a list of the most common drives accessible to Members:

1. The H:\ drive is the individual network drive. Disk space on this drive is to be used to store work related information. Each Member is allotted 500 megabytes of individual network drive space. If additional disk space is needed, please place a service request with your command's designated staff to submit an authorization request. Once approved for more allocated space you will be contacted by Systems Personnel.
2. The S:\ drive is the commandal drive. This drive serves as active file storage and file sharing within each command.

352.6.3 BACKUP SCHEDULE

All network drives are backed up nightly. Local drives on individual desktops and laptops are not backed up. Local drives typically include C:\, D:\, and E:\ drives. The "My Documents" folder is usually saved on a local drive, typically the C:\ drive on computers. Peripheral devices such as thumb drives (other names include jump drives or thumb drives) are not backed up. If a failure occurs on the local drives or on a thumb drive, there is the risk that files may not be retrievable.

352.6.4 PROCEDURES

Members should review the contents of their drives that they have access to and delete any files that are not allowed within this policy. Suggestions for reducing the size of the network drives include:

1. Remove personal files from all network drives.
2. Remove outdated files that are no longer needed or have been replaced by new files.
3. Review with the Departmental supervisor to identify any materials that should be removed from the Departmental drive. If there are old materials that should be archived, the Departments can send a request to the Help Desk to arrange for archiving to media.

Orange County Sheriff-Coroner Department

Orange County SD Policy Manual

Department Computer Use

352.6.5 RATIONALE & RESPONSIBILITIES

Network drive resources are provided to ensure safe and secure locations where Members may store current, work-related documents. Prudent use of this resource ensures that everyone has the storage they need to execute their daily tasks and maintain documents and files.

Users are expected to use Department resources in a responsible manner. Information Systems is responsible for ensuring that the storage resources are sufficient to meet the Member and Department needs. When an exception to this policy is granted, Information Systems is responsible for reviewing all requests for additional allotments and making appropriate adjustments as deemed essential to the operation of the Department.