

## Electronic Communications Policy

### 336.1 INTRODUCTION

With the spread of telecommunications throughout the modern work place, the Department recognizes that Members shall shift the ways they share ideas, transmit information and contact others. As Members are connected to outside resources via the Internet, their use of new tools and systems brings new responsibilities as well as opportunities.

The "Internet" or "The Net" is not a single network; rather, it is a group of thousands of individual networks, which have chosen to allow traffic to pass among them. The traffic sent out to the Internet may actually traverse several different networks before it reaches its destination. Therefore, users involved in this internetworking must be aware of the load placed on other participating networks.

As a user of the network, you may be allowed to access other networks and/or the computer systems attached to those networks. Each network or system has its own set of policies and procedures. Actions, which are routinely allowed on one network system, may be controlled, or even forbidden, on others. It is the user responsibility to abide by the policies and procedures of these other networks.

This policy covers official dissemination tools such as Electronic mail, Gopher, World Wide Web, FTP, LOCIS, WAIS, and the establishment and management of electronic discussion groups (Listservs and USENET Newsgroups).

This policy is interpreted through the following guidelines.

### 336.2 USE OF THE INTERNET BY SHERIFF-CORONER'S DEPARTMENT STAFF

The Internet provides access to a wide variety of information resources that can aid Department Members in the performance of their jobs. Examples of job-related use of the Internet at the Department include, but are not limited to: accessing external databases and files to obtain reference information or conduct research; corresponding with other municipal Members, including those outside of Orange County; communicating with fellow committee members in professional organizations; collaborating on articles and other writing; connecting to resources that provide information related to Department functions.

- **GUIDELINE #1:** Department Members may use the Internet for reasonable exploration and sharpening of skills in accordance with the conditions governing access to their work areas.

Members may use the Internet during work hours to enhance their knowledge of electronic information resources and sharpen information technology skills. Internet use provides cost-effective self-training opportunities. By encouraging reasonable exploration of the Internet at work, the Department builds a pool of Internet-literate Members who can guide and encourage other Members in using the Internet. (It shall be each commander's responsibility to define "reasonable exploration" for their respective division).

## *Electronic Communications Policy*

---

- **GUIDELINE #2:** Department Members must conform to the detailed "Standards of Conduct" which set out specific rules of etiquette for each of the available Internet vehicles.

OCSD Members have an obligation to learn about network etiquette (netiquette), customs and courtesies. Accepted procedures and guidelines should be followed when using electronic mail communications, participating in electronic mail discussion groups, using remote computer server, transferring files from other computers or disseminating information to others on the Internet. Members also have an obligation to be aware of computer security and privacy concerns and to guard against computer viruses.

- **GUIDELINE #3:** Use of the Internet by Department Members is a privilege, not a right, and may be revoked at any time for inappropriate conduct. All Department Members are responsible for complying with the policies, guidelines, and standards of conduct contained in this document. Violations may result in a revocation of Internet access privileges and other applicable penalties.

### **336.3 STANDARDS OF CONDUCT**

In General:

Department Members have an obligation to use their access to the Internet in a responsible and informed way, conforming to network etiquette, customs, and courtesies. Use of the Internet encompasses many different interconnected networks and computer systems. Many of these systems are provided free of charge by universities, public service organizations, and commercial companies. Each system has its own rules and limitations and guests on these systems have an obligation to learn and abide by the rules.

Users should identify themselves properly when using any Internet service. They should also be careful about how they represent themselves, given that what they say or do could be interpreted as Department opinion or policy. Users should be aware that their conduct could reflect on the reputation of the Department and its Members.

As noted in Guideline #3, Policy 343.2, use of the Internet is a privilege, which may be revoked at any time for inappropriate conduct. The user is ultimately responsible for his/her actions in accessing network services.

Examples of inappropriate conduct include but are not limited to:

1. Use of the Internet for unlawful activities
2. Use of abusive or objectionable language in either public or private messages
3. Viewing or sending obscene material
4. Misrepresentation of oneself or the Department
5. Sending chain letters
6. Using official dissemination tools to distribute personal information

# Orange County Sheriff-Coroner Department

## Orange County SD Policy Manual

### *Electronic Communications Policy*

---

7. Harassment in any form, including the persistent annoyance of others or interference in others work, including the sending of unwanted mail
8. Other activities that could cause congestion and disruption of networks and systems
9. Sharing of jokes

#### **336.4 APPROPRIATE USE: INTERNET ELECTRONIC MAIL AND FILE STORAGE AREAS**

1. Whenever you send electronic mail, your e-mail address is included in each mail message. You are responsible for all electronic mail originating from your userID. Use caution when revealing your address, credit card numbers, or phone number or those of others.
2. Attempts to read, delete, copy, or modify the electronic mail of other users are prohibited.
3. The content and maintenance of a user's electronic mailbox and shared file storage areas are the user's responsibility.
4. Check your electronic mail daily.
5. Be aware that electronic mail is not private communication because others may be able to read or access mail. Electronic mail may best be regarded as a postcard rather than as a sealed letter.
6. Delete unwanted messages or files immediately because they take up disk storage space.
7. Keep messages stored in electronic mailboxes to a minimum.
8. Use capitalization sparingly. Capitalizing long portions of a communication is considered SHOUTING! Use \*Asterisks\* or \_underscores\_ for emphasis.
9. Transfer to disks for future reference any messages or files to be saved.
10. It is the responsibility of the user to scan any downloaded files for viruses

#### **336.5 APPROPRIATE USE: ELECTRONIC DISCUSSION GROUPS**

Members who participate in electronic discussion groups (listservs, Usenet newsgroups, etc.) should learn and abide by the rules and etiquette of those groups. Some general guidelines are:

1. When not officially representing the Department, if the message could be perceived as Department business or opinion, add a disclaimer to the message. An example of a disclaimer is:
  - (a) "The opinions expressed here are my own and do not necessarily represent those of the Sheriff-Coroners Department."
2. Keep messages short and to the point. Generally, limit messages to one subject.
3. Act in a professional and courteous manner. Avoid gossip and remember that statements about others may find their way back to them. Be patient with new users. Be clear and concise. Re-read messages before sending them to be sure that they will not be misunderstood. Read all messages carefully before responding.

## *Electronic Communications Policy*

---

4. Be aware of the potential audience in any discussion group and address them accordingly.
5. Be careful when using sarcasm and humor. Identify intended humor with standard statements (e.g., "only joking folks" or with symbols (e.g.,-) smiley face.
6. Limit line length to fewer than 80 characters, because many systems cannot display longer lines.

### **336.6 APPROPRIATE USE: TELNET (USING REMOTE COMPUTERS)**

When using TELNET to access remote computer systems, users should remember that they are guests on another institution's machine. To help ensure that other Internet users have access to the same information in a timely manner, remote users should observe a few basic courtesies:

1. Logoff a remote computer system when finished. Maintaining a connection that is not actively being used may prevent others from connecting to that system.
2. Read or obtain instructions or documentation files when using a system for the first time.
3. Be aware of time and resource limitations of remote systems. Adhere to any stated restrictions.

### **336.7 APPROPRIATE USE: FTP (FILE TRANSFER PROTOCOL)**

When using FTP, users are guests on other systems. To ensure that other Internet users have access to the information, a few basic guidelines should be followed:

1. Login as anonymous and respond to the PASSWORD prompt with your electronic mail address, unless the system specifies otherwise. (If your e-mail address causes an error, enter GUEST for the password). Logoff the remote computer system when finished.
2. Avoid transferring files during peak business hours for the remote system, whenever possible.
3. Respect copyright and licensing agreements of transferred files.
4. It is the responsibility of the user to scan any downloaded files.

### **336.8 APPROPRIATE USE: PROVIDING ELECTRONIC INFORMATION**

To ensure that information is disseminated properly, Members should observe a few basic guidelines:

1. Obtain the appropriate approvals, prior to placing any information on the Internet.
2. Restrict information that should only be available to Department Members.
3. Make every attempt to ensure that the information being provided is accurate and is kept up to date.
4. Never use official dissemination tools to distribute personal information.

# Orange County Sheriff-Coroner Department

Orange County SD Policy Manual

## *Electronic Communications Policy*

---

### **336.9 SHERIFF-CORONER'S DATA NETWORK (SDN)**

The Sheriff-Coroner's Data Network (SDN) is under the administration of the Technology Division.

The Sheriff's Data Network is a high-speed network connecting all Department facilities, participating Orange County municipal police Departments and other state and federal law enforcement agencies. The SDN provides connectivity between desktop computers throughout the Department, as well as connection to other networks such as the Internet, C.L.E.T.S and the Statewide Integrated Narcotics System. The SDN currently provides access to a wide range of applications, such as AJS, LARS, AWSS, ACS, ROS, Cal Gangs (formerly GREAT) and the Department's Intranet Server. For an up-to-date list of applications available on the Sheriff's Data Network, contact the Technology Division help-desk.

### **336.10 ELECTRONIC COMMUNICATIONS**

The following sections of the Department's Manual of Policy and Procedures set forth the Department policies for electronic communications including activity involving the Internet, Sheriff's Data Network, DOJ Data Interface Controller, local area networks, individual personal computers, and access to data stored in local, state and federal computer systems. Electronic mail and faxes, which are transmitted over both the Internet and Sheriff's Data Network, are subject to all provisions of this policy. The Technology Division is responsible for the administration of electronic communications via the Internet, Sheriff's Data Network and Orange County Intranet.

1. SHERIFF-CORONER'S LOCAL AREA NETWORKS
  - (a) OCSD LANs are defined as Information Resources (PCs, Printers etc.) interconnected for the purpose of sharing the resources and information within an isolated facility in accordance to OCSD I/S standards.
2. B. SHERIFF-CORONER'S WIDE-AREA-NETWORK
  - (a) Group of LANs interconnected for the purpose of sharing resources and information with other OCSD Commands and External networks in accordance to OCSD I/S standards and security policies.

### **336.11 DEPARTMENT STANDARDS FOR HARDWARE AND O.S.**

The Technology Division is responsible for selecting and purchasing the standard desktop software suite for all Department computers on the Wide-Area-Network and for administration of the software on computers connected to the Sheriff's Data Network.

The standard desktop productivity software for the Department's Wide-Area-Network is Microsoft Outlook for electronic mail and calendar, Microsoft Internet Explorer for Internet and the MS Office Suite for word processing, spreadsheet and presentation. All Department Members shall use the Department's selected desktop software unless critical functionality is not available through the application. Specialized software needs shall be assessed on an individual basis and not withstanding technical conflicts installed with Commander approval. The Technology Division purchases, maintains, and installs desktop software for all Department WAN computers.

1. INSTALLING LICENSED SOFTWARE

# Orange County Sheriff-Coroner Department

Orange County SD Policy Manual

## *Electronic Communications Policy*

---

- (a) Members are prohibited from installing or maintaining unlicensed software on any Department computer. Members who wish to install licensed software on a Department computer must have authorization from their unit commander and the Technology Division. The software installation and record of the installation will be the responsibility of the Technology Division. A copy of the software license must be provided to the Technology Division prior to the installation.
2. BACKING UP FILES
- (a) It is strongly recommended that users store important data files in their personal folder in the unit file server. These files shall be "backed up" daily to prevent loss of information. They cannot be accessed by other users and offer the highest degree of individual security. Any files stored on the local drive ("C" drive) of the computer are not secure against access by other users and will not be backed up to prevent loss of information. During routine maintenance computers may be replaced or hard drives erased without notice to the user. Data contained on the local drive ("C" drive) of these machines/hard drives may be lost to the user.

*Members shall be allocated space for the storage of their files in the personal folder on the server, however, Members are encouraged to delete or archive personal, unused or obsolete data stored in Department computers (local hard drive or assigned space on server) as soon as practical. When maximum storage capacity is reached, Members shall be advised to remove files.*

### **336.12 PERMISSIBLE USE**

The use of any Department computer resource is restricted to those activities related to Department business. Use of computers and electronic communications by Members is authorized in support of the law enforcement mission of the Department and the administrative functions that support that mission. Department Members and other authorized users shall adhere to this policy as well as the guidelines set forth in the county Electronic Data Communications and Intranet/Internet Policies.

Members are expected to abide by the standards of conduct delineated in other volumes, chapters and sections of the Department's Manual of Policy and Procedures as they may be applied to the use of electronic communications and use and release of information.

### **336.13 AUTHORIZED PERSONS**

Access to computers, networks, and electronic communications on behalf of the Department is limited to Department Members, reserves, volunteers, county Members, and expanded SDN participating police agency Members, contractors, subcontractors, and their Members conducting Department business. Hereafter in this policy, authorized persons shall be referred to as Member(s). Unauthorized persons, including inmates, shall not be permitted to access or otherwise utilize computers or network equipment under the direction or permission of a Member.

# Orange County Sheriff-Coroner Department

## Orange County SD Policy Manual

### *Electronic Communications Policy*

---

#### **336.14 SYSTEM USE**

Members are expected to use electronic communications and network systems with a high degree of professional and personal courtesy. Members must ensure that the tone and content of electronic communications are businesslike and exclude inflammatory remarks or inappropriate language.

##### 1. ELECTRONIC MAIL

- (a) Although e-mail senders have no rights of privacy, Members should respect the privacy of E-mail delivered to them. Members shall not forward or otherwise disclose the contents of electronic messages with the intent to embarrass or otherwise harm the sender. If it is an issue that could cause embarrassment, it does not belong on e-mail. This does not prohibit the receiver of e-mail from divulging the contents of electronic communications messages to a Member's supervisor or to Department management.
- (b) Members who receive an electronic communication intended for another person shall attempt to notify the sender as soon as possible of the error.
- (c) Members who are authorized users of e-mail are responsible for reading their electronic mail as frequently as possible, or notify their supervisor that they are unable to read e-mail.

##### 2. LOGGING OFF

- (a) To enhance security and ensure that shared computers are available to all Members, users shall logoff their computer when away from their workstation and at the end of the work shift.
- (b) All computers connected to the Sheriff-Coroner's Data Network must remain "on," at all times after hours in order to provide after-hours maintenance. After hours or when a Member is away from his or her computer it must be "logged off" but remain turned on.

##### 3. PROHIBITED DEVICES

- (a) All dial-up connections, modem connections, and electronic communication devices are prohibited on the Sheriff's Wide-Area-Network. Stand-alone machines not connected to WAN may have dial-up or other connections with Commander approval and Technology Division review.
- (b) The Technology Division will ensure that all requests for any of the above connections are reviewed by knowledgeable staff. The purpose of the review will be to evaluate the risk and potential for illegal access to Departmental systems, stored records, and confidential information. These findings will be reported to the requesting Commander so that an informed decision can be made.

##### 4. GUIDELINES

- (a) Department Members who use any computer/modem connection provided by the Department shall adhere to the following guidelines:
  - (a) Only those persons authorized by the appropriate Commander/Director shall utilize Department dial-up computer connections.

# Orange County Sheriff-Coroner Department

Orange County SD Policy Manual

## *Electronic Communications Policy*

---

- (b) Authorized users of Department computer dial-up connections shall only use those connections for Department business.
- (c) Use of dial-up connections for other than Departmental business shall be subject to disciplinary action.

Nothing in this section is to be constructed as prohibiting lawful criminal investigation on the Internet or research related to such investigations nor is it intended to prohibit research beneficial to the Orange County Sheriff-Coroner's Department or the County of Orange.

### **336.15 PRIVACY**

Department Members and other authorized users should not have any expectation of privacy when using computer and network systems. All electronic files and e-mail in Department systems are considered the property of the Department and may be accessed at any time by authorized supervisory/management personnel without the Member's permission or notification.

The Department reserves the right to engage in monitoring electronic communications such as e-mail, faxes, computer files, and networks, including the inspection of files created by Members and stored in Department systems, to ensure that the public resources are appropriately used for county related business, including audits and Member supervision.

Department Members who are authorized to access to the Internet World Wide Web shall be monitored to ensure that Internet access is used for Department business. Internet addresses accessed by each user shall be electronically monitored, summarized and forwarded to the Member's Commander when suspect traffic to Internet sites is found.

The Technology Division network administrators may view the contents of electronic messages and files during the administration of the network computers.

Electronic communications and data may be subject to disclosure to third parties in response to the "Public Records Act" or other lawful court orders.

### **336.16 CONFIDENTIALITY**

The Department cannot control the final disposition of electronic communications once they have been delivered. Members should be cautioned that any electronic message might be forwarded or printed without the sender's knowledge.

Department Members should be aware that e-mail could be illegally intercepted enroute to its destination. No confidential communications shall be made via e-mail unless encrypted with encryption software approved by appropriate the Technology Division staff.

### **336.17 SECURITY**

Only Department Members or other persons authorized by the Technology Division may access the Sheriff's Data Network. Those authorized shall be assigned a logon identification code (i.e., USERID or ID). Only the authorized owner of the ID is permitted to use the ID. Those assigned an ID shall be required to select a password. Members shall not disclose their computer passwords

# Orange County Sheriff-Coroner Department

Orange County SD Policy Manual

## *Electronic Communications Policy*

---

to another person, except as required under this policy. Members are responsible to keep their passwords secret and to change them if compromised. Any electronic communications sent using an Member's USERID and password is prima facie evidence the Member assigned the USERID and password generated the communications. In other words, if your username and ID appears, it is assumed you forwarded the message so do not give anyone your user name or password.

### 1. USERID

- (a) Members shall not share common USERID and passwords for any computer system, except as required for training. Any person who has knowledge of individuals who are sharing common USERID and passwords shall immediately notify their unit supervisor. Members shall have only one network, e-mail, and fax account. Only the Technology Division shall establish user network, electronic mail, fax, Internet, and remote access accounts.

### 2. PASSWORDS

- (a) The password selected by Members shall not contain their first name, middle name, last name, or Member number. Passwords must be six characters with at least one non-alphabetic character. Members cannot reuse the most recently used passwords.
  1. The network shall permit only five (5) attempts of a person's USERID and password before locking out network access.
- (b) Members shall report to their immediate supervisor, in writing, any violations of electronic communications policy as set forth in the Manual of Policy and Procedures.

### **336.18 APPROVED ACCESS**

Members are required to keep the personal information section (properties) of the Outlook (e-mail) address book up-to-date. This includes title, work address, unit of assignment, work location, work phone number, and fax number. Optional items include mobile phone number and pager number.

Department Members may have access to the Internet World Wide Web, subject to the approval of their Commander.

Various levels of system access shall be granted on an as needed basis determined by Commanders.

Individuals needing access to the files of another, when the Member is unavailable, must obtain approval from the concerned Member's supervisor or unit commander. Upon authorization, the Technology Division shall provide and record the access given.

### **336.19 PROHIBITIONS**

Members shall not add, alter, copy, damage, delete, move, modify, tamper with, or otherwise use or affect any data or software, computer, computer system, or computer network in order to either:

1. Devise or exclude any scheme or artifice to defraud, deceive, destroy or extort, wrongfully control, or obtain money, property or data.

# Orange County Sheriff-Coroner Department

Orange County SD Policy Manual

## *Electronic Communications Policy*

---

2. Disrupt or cause the disruption of computer or network services or deny or cause the denial of computer or network services to an authorized user of a Department computer, computer system, or computer network.
3. Assist in providing access to unauthorized persons to any data, software, programs, and computer system or computer network.

Unless specifically authorized by the Technology Division, Department Members shall not install, connect to, move, change, modify, disconnect, or tamper with any data circuit, router, switch, hub, data jack, data cable, server, or other data communications equipment, or software or assist any unauthorized person in gaining access to data circuits, routers, switches, hubs, data jacks, data cables, servers, or other data communications equipment, devices, or software.

### **336.20 AUTHORIZATION REQUIRED**

Members shall not do any of the following without the required authorization:

1. Access or allow access to another to obtain, alter or prevent access to stored electronic communications.
2. Use electronic communications to capture or open electronic communications of another or access files without permission of the owner.
3. Damage hardware, software, or other communications equipment or interfere with functionality.
4. Attempt to breach any security measures on any electronic communications system or attempt to intercept any electronic communication transmission.
5. Modify or delete any file, folder, or system audit, security or ownership records or time stamp with the intent to misrepresent true system audit records.
6. Access the files belonging to another for non-business purposes.
7. Use someone else's USERID, password or access another person's files or retrieve stored communications without authorization.
8. Modify the hardware or software configuration on any computer.
9. Modify or delete the automatic scan for computer viruses.
10. Use electronic communications to transmit (upload) or knowingly receive (download):
  - (a) Any communication violating any applicable laws, regulations or policies.
  - (b) Proprietary or confidential Department information.
  - (c) Chain letters.
  - (d) Material that would be offensive to a reasonable person.
11. Transmit any electronic message in violation of file size restrictions.
12. Use Department computer equipment or network to send or receive electronic communications for non-Department business.

# Orange County Sheriff-Coroner Department

Orange County SD Policy Manual

## *Electronic Communications Policy*

---

13. Use computers, networks, or electronic communications to infringe on the copyright or other intellectual property rights of the county or third parties.
14. Send or receive commercial software in violation of its license agreement.
15. Copy personal files programs or images into any Department computer without authorization from their bureau captain.
16. Send anonymous messages or represent oneself as someone else, real, or fictional or send messages or images, which are defamatory, fraudulent, threatening, harassing, sexual, or contain derogatory racial or religious content.
17. Establish any hidden or misidentified links on any web page.
18. Send or forward messages that have been altered in order to deceive the receiver as to the original content.
19. Use Department computers, networks, software, or electronic communications for personal financial, commercial, political, or other personal use.
20. Use electronic communications to intimidate, embarrass, cause distress, or otherwise force unwanted attention upon others or to interfere with the ability of others to conduct Department business or create a hostile work environment.
21. Use electronic communications in competition with commercial services to individuals or organizations outside the Department.
22. Use electronic communications for the purposes of gambling, including but not limited to, lotteries, sports pools, and other personal wagering.
23. Give out Member personal information such as home address and/or telephone numbers.
24. Modify or update the Department "Web Page" without prior approval of the appropriate Assistant Sheriff.

### **336.21 CALIFORNIA DEPARTMENT OF JUSTICE ADMONISHMENT**

As an Member of the Orange County Sheriff-Coroner's Department, you may have access to confidential criminal record and/or Department of Motor Vehicles record information, which is controlled by statute. Misuse of such information may adversely affect the individual's civil rights and violates the law. Penal Code Section 502 prescribes the penalties relating to computer crimes. Penal Code Sections 11105 and 13300 identify who has access to criminal history information and under what circumstances it may be released. Penal Code Sections 11140 11144 and 13301 13305 prescribe penalties for misuse of criminal history information. Government Code Section 6200 prescribes the felony penalties for misuse of public records and CLETS information. Penal Code Sections 11142 and 13303 state:

*"Any person authorized by law to receive a record or information obtained from a record who knowingly furnishes the record or information to a person not authorized by law to receive the record or information is guilty of a misdemeanor."*

# Orange County Sheriff-Coroner Department

Orange County SD Policy Manual

## *Electronic Communications Policy*

---

California Vehicle Code Section 1808.45 prescribes the penalties relating to misuse of Department of Motor Vehicles record information.

Any Member who is responsible for such misuse is subject to disciplinary action. Violations of this law may also result in criminal and/or civil actions.

### **336.22 DATA COMMUNICATIONS MANAGEMENT**

The Technology Division is responsible for overall access and administration of electronic data communications policy and procedures for any traffic occurring over the Sheriff-Coroner's Data Network, OCATS, CLETS, and Department ALPR. In this role, the Technology Division shall:

1. Review and approve requests for access to the Sheriff-Coroner's Data Network, OCATS, CLETS, and Department ALPRs. Requests for such access should be made to the Technology Division help desk accompanied by written Commander approval.
2. Review and act on all requests to receive e-mail. Requests for e-mail should be made to the Technology Division help desk.
3. Review and act on requests from Department users to install new equipment, hardware or software connected to the Sheriff-Coroner's Data Network. Such requests should be made to the Technology Division help desk.
4. Review requests and provide Internet access for individual Department Members. Requests for such access must be submitted on a Department memo (attachment #3) from the requestor's Commander/Director to the Technology Division Director. The Technology Division is responsible for maintaining a list of authorized Internet users.
5. Specify the software required for usage with computers connected to the Sheriff-Coroner's Data Network and ensure its usage on all such computers.
6. Establish the standards and purchase all electronic communications equipment including personal computers, printers, scanners, and network equipment for the Department, as such equipment relates to the wide area network.
7. Establish and purchase the standard software suite for Department computers, including desktop and network operating systems, virus scanning, e-mail, faxes, word processing, spreadsheet, graphics, database, and network management software.
8. Review and act on requests to use encryption technology by Department Members.

### **336.23 NETWORK / FIELD SUPPORT & HELP DESK**

The Sheriff-Coroner's Data Network provides 24-hour support for system outages related to the mainframe. A system outage is defined as the inability to access mission critical services such as AJS, WPS, or CLETS/OCATS. If this occurs contact Information Services Help Desk at [REDACTED]. All non-mission critical system or computer related problems would be processed on the next business day. Routine service and support is currently not available on a 24-hour basis. Members should call or e-mail the Technology Division help desk to report hardware, software, and other problems encountered while utilizing an SDN connected device.

# Orange County Sheriff-Coroner Department

Orange County SD Policy Manual

## *Electronic Communications Policy*

---

### **336.24 OCSD USER AUTHORIZATION AND ACKNOWLEDGMENT OF POLICIES AND GUIDELINES**

Members shall be responsible for reading and signing the Department "User Acknowledgment of Electronic Communications Policy" form (Section 343.25) before obtaining authorization to access the Sheriff-Coroner's Data Network. The Department form requires a counter signature by the user's supervisor at the rank of sergeant or higher.

### **336.25 USER ACKNOWLEDGMENT OF ELECTRONIC COMMUNICATIONS POLICY**

I understand that the Orange County Sheriff-Coroner's Department requires each user, who has access to automated data communications, be responsible for adhering to its electronic communications policy sections as set forth in the Manual of Policy and Procedures. I have received a copy of these Policy and Procedures.

I understand that I must not have an expectation of privacy when using county electronic communications and acknowledge that my electronic communications may be monitored at any time by authorized Members.

By signing this form, I agree to abide by all policies, including state statutes relating to electronic communications and use of information, and understand that I will be held accountable for my actions and that disciplinary actions may result from not abiding by these policies. I also understand authorized persons, including supervisors, auditors and investigators may access any equipment, software and files at any time.

---

User Name (PRINT) User Signature Date

As a supervisor, by my signature, I acknowledge my responsibility to have provided the electronic communications policies, to the above user. I also acknowledge that I am responsible for ensuring that the above user, whom I supervise, has read and understands this policy.

---

Supervisor's Name (PRINT) Supervisor's Signature Date