

# Information Technology Use

## 321.1 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.

### 321.1.1 DEFINITIONS

Definitions related to this policy include:

**Computer system** - All computers (on-site and portable), electronic devices, hardware, software, and resources owned, leased, rented or licensed by the Garden Grove Police Department that are provided for official use by its members. This includes all access to, and use of, Internet Service Providers (ISP) or other service providers provided by or through the Department or department funding.

**Hardware** - Includes, but is not limited to, computers, computer terminals, network equipment, electronic devices, telephones, including cellular and satellite, pagers, modems or any other tangible computer device generally understood to comprise hardware.

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

**Temporary file, permanent file or file** - Any electronic document, information or data residing or located, in whole or in part, on the system including, but not limited to, spreadsheets, calendar entries, appointments, tasks, notes, letters, reports, messages, photographs or videos.

## 321.2 POLICY

It is the policy of the Garden Grove Police Department that members shall use information technology resources, including computers, software and systems, that are issued or maintained by the Department in a professional manner and in accordance with this policy.

## 321.3 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to emails, texts, or anything published, shared, transmitted, or maintained through file-sharing software or any internet site that is accessed, transmitted, received, or reviewed on any department computer system.

The Department reserves the right to access, audit, and disclose, for whatever reason, any message, including attachments, and any information accessed, transmitted, received, or reviewed over any technology that is issued or maintained by the Department, including the department email system, computer network, and/or any information placed into storage on any department system or device. This includes records of all keystrokes or Web-browsing history made at any department computer or over any department network. The fact that access to a database, service, or website requires a username or password will not create an expectation of privacy if it is accessed through department computers, electronic devices, or networks.

# Garden Grove Police Department

## Policy Manual

### *Information Technology Use*

---

The Department shall not require a member to disclose a personal username or password for accessing personal social media or to open a personal social website; however, the Department may request access when it is reasonably believed to be relevant to the investigation of allegations of work-related misconduct (Labor Code § 980).

Any personal use of department computers and software must be approved by a department manager and use must be on non-city time. Department computers shall not be used for any outside business activity as set forth in Municipal Code 2.02.050. Approval for personal use of department computers and software may be revoked at any time without prior notice.

No personal data, information, or software may be installed or stored on the Department's system or individual personal computers.

The Department's Information Systems Technician or other designated department representative is authorized to copy and/or delete any non-city approved or personal software, hardware, data or information on the department computer system.

#### **321.4 RESTRICTED USE**

Members shall not access computers, devices, software or systems for which they have not received prior authorization or the required training. Members shall immediately report unauthorized access or use of computers, devices, software or systems by another member to their supervisors or Division Lieutenants.

Members shall not use another person's access passwords, logon information and other individual security data, protocols and procedures unless directed to do so by a supervisor.

Account passwords for Department and City systems should not be shared or re-used with other systems outside the department.

##### **321.4.1 SOFTWARE**

To reduce the risk of a computer virus or malicious software, 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.

When related to criminal investigations, software program files may be downloaded only with the approval of the information systems technology (IT) staff and with the authorization of the Chief of Police or the authorized designee.

No member shall knowingly make, acquire or use unauthorized copies of computer software that is not licensed to the Department while on department premises, computer systems or electronic devices. Such unauthorized use of software exposes the Department and involved members to severe civil and criminal penalties.

Introduction of software by members should only occur as part of the automated maintenance or update process of department- or City-approved or installed programs by the original manufacturer, producer or developer of the software.

# Garden Grove Police Department

## Policy Manual

### *Information Technology Use*

---

Any other introduction of software requires prior authorization from IT staff and a full scan for malicious attachments.

Programs developed by employees while using department software and/or equipment shall remain the property of the department.

Requests to install software must be made online through IT portal or E-mail and the requester must acknowledge receipt of the memorandum that lists the conditions for software installation.

The Department's Information Systems Technician shall maintain a record of software installed on the network and each computer. The information shall include the program name, software manufacturer, revision number, whether it is an upgrade, the software license or registration number and the date of purchase.

#### 321.4.2 HARDWARE

Access to technology resources provided by or through the Department shall be strictly limited to department-related activities. Data stored on or available through department computer systems shall only be accessed by authorized members who are engaged in an active investigation or assisting in an active investigation, or who otherwise have a legitimate law enforcement or department-related purpose to access such data. Any exceptions to this policy must be approved by a supervisor.

Department computers are not to be considered personal property and are not to be used as such. No employee shall use, access, or attempt to access any computer, computer network, computer software program, computer language, computerized database or computer storage device, or any part of the computer without authorization.

The Support Services Bureau Commander shall serve as the Department's Network Administrator. The Department's Information Systems Technician will be designated as the Department's PC Coordinator. The PC Coordinator will process requests to purchase and install new software and hardware and ensure that PC-related Department property is recorded appropriately. Only the Department's Information Systems Technician or his/her designee will be authorized to install and delete software or install and remove hardware. The Department's Information Systems Technician is authorized to delete any non-approved hardware, software, or other information from any computer.

No employee shall access and without permission take, copy, print or make copies of any data from any computer, computer network, computer software program, computer language, computerized database or computer storage device, including any supporting documentation whether existing or residing internally or externally to these systems.

No employee shall intentionally or willfully and without permission delete, damage, destroy or adversely alter any data or software program in the computer network or any computer.

No employee shall attempt to identify any access codes or passwords. Nor will any employee distribute or provide any passwords or access codes. However, nothing in this section shall restrict

# Garden Grove Police Department

## Policy Manual

### *Information Technology Use*

---

the rights of the department to access and inspect any and all data derived from or stored within the computer network or any department computer.

No employee shall protect their personal computer BIOS (Basic Input/Output System) through the use of passwords. No employee shall alter any of the network operating systems. Each employee shall ensure that their directories, data, and documents are protected by the use of passwords.

No employee shall refuse to furnish copies of, or relinquish computer files, records, archives or data stored on the network or any department computer storage device, file, record, archive or data.

Upon request of their supervisor, all employees shall provide any password or other code or information that will facilitate access to any data on information stored on Department equipment.

#### **321.4.3 INTERNET USE**

Internet access provided by or through the Department shall be strictly limited to department-related activities. Internet sites containing information that is not appropriate or applicable to department use and which shall not be intentionally accessed include but are not limited to adult forums, pornography, gambling, chat rooms, and similar or related internet sites. Certain exceptions may be permitted with the express approval of a supervisor as a function of a member's assignment.

Downloaded information shall be limited to messages, mail, and data files.

#### **321.4.4 OFF-DUTY USE**

Members shall only use technology resources provided by the Department while on-duty or in conjunction with specific on-call assignments unless specifically authorized by a supervisor. This includes the use of telephones, cell phones, texting, email or any other "off the clock" work-related activities. This also applies to personally owned devices that are used to access department resources.

Refer to the Personal Communication Devices Policy for guidelines regarding off-duty use of personally owned technology.

#### **321.5 PROTECTION OF AGENCY SYSTEMS AND FILES**

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

Members shall ensure department computers and access terminals are not viewable by persons who are not authorized users. Computers and terminals should be secured, users logged off and password protections enabled whenever the user is not present. Access passwords, logon information, and other individual security data, protocols, and procedures are confidential information and are not to be shared. Password length, format, structure, and content shall meet the prescribed standards required by the computer system or as directed by a supervisor and shall be changed at intervals as directed by IT staff or a supervisor.

# Garden Grove Police Department

## Policy Manual

### *Information Technology Use*

---

It is prohibited for a member to allow an unauthorized user to access the computer system at any time or for any reason. Members shall promptly report any unauthorized access to the computer system or suspected intrusion from outside sources (including the internet) to a supervisor.

#### **321.6 INSPECTION OR REVIEW**

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

Reasons for inspection or review may include, but are not limited to, computer system malfunctions, problems or general computer system failure, a lawsuit against the Department involving one of its members or a member's duties, an alleged or suspected violation of any department policy, a request for disclosure of data, or a need to perform or provide a service.

The IT staff may extract, download or otherwise obtain any and all temporary or permanent files residing or located in or on the department computer system when requested by a supervisor or during the course of regular duties that require such information.

#### **321.7 RELATED PROCEDURES**

See INFORMATION TECHNOLOGY USE PROCEDURES in the Garden Grove PD Procedures Manual.