Department Computer Use

342.1 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.

342.1.1 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 Pasadena 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.

342.2 POLICY
It is the policy of the Pasadena 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.

342.3 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.
Department Computer Use

However, the Department may not require a member to disclose a personal username or password or open a personal social website, except when access is reasonably believed to be relevant to the investigation of allegations of work-related misconduct (Labor Code § 980).

342.4 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 Watch Commanders.

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.

342.4.1 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 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.

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

342.4.2 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.
342.4.3 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.

342.4.4 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.

342.5 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.

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.

342.6 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
Department Computer Use

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.

342.7 RESPONSIBILITIES

(a) Section Supervisors will ensure:
   1. That personnel are trained to operate computer systems under their division's responsibility; and
   2. That Department personnel follow the rules of all licensed computer programs and systems in use within the Unit.

(b) Section lieutenants or Administrators and users of Department computers, equipment, software, and supplies will care for and protect these items. This includes maintaining adequate backup files and training replacement personnel in the operation and maintenance of computer systems within their respective sections.

(c) Section Lieutenants or Administrators will ensure that Department personnel follow the section rules of all licensed computer programs and systems in use within the Section. The Strategic Services Commander is authorized to conduct periodic equipment, software, and supply inspections, where and when necessary. Discovery of unauthorized software will result in its removal from the system and notification of such finding to the Chief of Police. A copy of this report will be given to the Section Administrator, who will then prepare a written response to the Chief of Police via the chain of command.

342.8 AUTHORIZED SOFTWARE

(a) Authorized software are those computer programs:

   1. Approved for purchase or acquisition by the City;
   2. Procured by individuals using personal funds and licensed, registered, or authorized to be installed on a Department computer. Proof of such permission must be in the form of personal possession of original disks, manuals and licenses. Installation and use must comply with the manufacturer's license;
   3. Equipment, procedures, texts, or publications provided to the Department through the Strategic Services, or Chief of Police.
   4. Equipment, procedures, texts, or publications provided to the Department through the Technical Services section, or Chief of Police. All material is properly maintained and accounted for. All equipment, software, publications, textbooks, etc. purchased through the use of City or Department authorized funds (budgeted and unbudgeted)
are the property of the City of Pasadena and the Pasadena Police Department. Such property will be available for use by all trained and authorized members of the Department.

(b) When personal computer related equipment is provided by members of the Department for personal use with Department software or equipment, each will be clearly labeled as such.

342.9 TRAINING

(a) The Technical Services Administrator will assist the Department Training Unit in the establishment of computer related training courses. In addition, the Technical Services Section will:

1. Coordinate the establishment of a training plan for the use of personal computers and automation within the Department. Such a plan will be coordinated with the PPD Training Unit, and training offered by City Department of Information Technology (DoIT).

2. Recommended training for personnel involved in the use of police systems. Training will be sufficient to provide emergency backup procedures to personnel within the Communications Section, and will be done with the coordination of the Communications Section Administrator.

342.10 REFERENCE