



## Department Technology Use

### 342.1 PURPOSE AND SCOPE

This policy describes the use of Department computers, software and systems.

#### 342.1.1 PRIVACY POLICY

Any employee utilizing any computer, electronic storage device or media, Internet service, telephone 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 employee, sender and recipient of any communications utilizing such service might otherwise have, including as to the content of any such communications. 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.

### 342.2 DEFINITIONS

Definitions related to this policy include:

**Computer System** -Includes all computers (on-site and portable), hardware, software and resources owned, leased, rented or licensed by the Peoria Police Department that are provided for use by Department employees.

**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** -Includes 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 or messages.

### 342.3 SYSTEM INSPECTION OR REVIEW

There is no expectation of privacy regarding files contained in or on Department computers or systems. A Department designee 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, whether such inspection or review is in the ordinary course of his/her supervisory duties or based on cause.

When requested by an employee's supervisor, or during the course of regular duties requiring such information, a member 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.

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 employee

# Peoria Police Department

## Policy Manual

### *Department Technology Use*

or related to the employee's duties, an alleged or suspected violation of any Department policy, request for disclosure of data, or a need to perform or provide an agency service.

#### **342.4 AGENCY PROPERTY**

All information, data, documents and other entries initiated on any of the agency's computers, whether downloaded or transferred from the original agency computer, shall remain the exclusive property of the Information Technology Department and shall not be available for personal or non-Department use without the express written authorization of the IT Director.

#### **342.5 UNAUTHORIZED DUPLICATION OF SOFTWARE**

City of Peoria users may not duplicate any licensed software or related documentation for use either on City of Peoria premises or elsewhere unless the City of Peoria is expressly authorized in writing to do so by agreement with the licensor. The Information Technology Department creates all authorized duplicate media and retains the master copy.

To reduce the risk of an agency computer virus infection, employees are not permitted to install personal copies of any software onto the computers owned or operated by the Department.

No employee shall knowingly make, acquire or use unauthorized copies of computer software that is not licensed to the Department while on Department premises or on a Department computer system. The Department and individuals can be subject to civil damages per title copied, along with criminal penalties including fines and imprisonment.

#### **342.6 INTERNET USE**

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

An Internet site containing information that is not appropriate or applicable to Department use and that shall not be intentionally accessed include, but is not limited to, adult forums, pornography, chat rooms and similar or related websites. Certain exceptions may be permitted with the approval of a supervisor as a function of an assignment.

Downloaded information shall be limited to messages, mail and data files. No copyrighted and/or unlicensed software program files may be downloaded without authorization of the Information Technology (IT) Department or, when related to criminal investigations, the Chief of Police or a designee.

Employees shall report any unauthorized access to the system or suspected intrusion from outside sources (including the Internet) to a supervisor.

# Peoria Police Department

## Policy Manual

### *Department Technology Use*

#### **342.7 INTRODUCTION OF SOFTWARE**

Introduction of software requires prior authorization by the IT Department. No software may be installed on any City owned or leased computer without prior written approval by the Information Technology Department and without being registered to the City of Peoria.

#### **342.8 PROTECTION OF DEPARTMENT SYSTEMS AND FILES**

All employees 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 an employee to allow an unauthorized user to access the system at any time or for any reason.