# Information Technology Use

## 338.1 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.

### 338.1.1 DEFINITIONS

**Computer system** - All computers (on-site and portable), electronic devices, hardware, software, networks and resources owned, leased, rented or licensed by the Yolo County Probation Department that are provided for official use by its employees. 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 computer system including, but not limited to, spreadsheets, calendar entries, appointments, tasks, notes, letters, reports, messages, photographs or videos.

**Social Media -** Electronic service or account, or electronic content, including but not limited to videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations for the purpose of social networking.

## 338.2 POLICY

It is the policy of the Yolo County Probation Department that employees 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.

## 338.3 PRIVACY EXPECTATION

Employees forfeit any expectation of privacy with regard to emails, texts or any materials or writings 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, or hardware.

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 system and/or any information placed into storage on any Department system or device. This includes records of all keystrokes or Web-browsing history made using any Department computer system, network or hardware. The fact 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, hardware, electronic devices or networks.

However, the Department may not require an employee to disclose a personal username or password or open a personal social media website, except when access is reasonably believed to be relevant to the investigation of allegations of employee misconduct or employee violation of applicable laws and regulations. (Lab. Code § 980.)

## 338.4 RESTRICTED USE

Employees shall not access computers, devices, software or systems for which they have not received prior authorization or the required training. Employees shall immediately report unauthorized access or use of computers, devices, software or systems by another employee to their Supervisor..

Employees 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.

### 338.4.1 SOFTWARE

Employees 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, employees shall not install any unlicensed or unauthorized software on any Department computer. Employees shall not install personal copies of any software onto any Department hardware.

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 Probation Officer or the authorized designee.

No employee 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 employees to severe civil and criminal penalties.

Introduction of software by employees should only occur as part of the automated maintenance or update process of Department or County-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.

### 338.4.2 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 employees 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.

### 338.5 PROTECTION OF AGENCY SYSTEMS AND FILES

a. All employees 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.

b. Employees shall ensure Department computers and access terminals are not viewable by persons who are not authorized users.

c. Computers and terminals should be secured, users logged off and password protections enabled whenever the user is not present.

d. Access passwords, logon information and other individual security data, protocols and procedures are confidential information and are not to be shared.

e. 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.

f. It is prohibited for an employee to allow an unauthorized user to access the computer system at any time or for any reason. Employees shall promptly report any unauthorized access to the computer system or suspected intrusion from outside sources (including the Internet) to a Supervisor.

### 338.6 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 or 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 employees or an employee'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.