

Computer Use

Department Technology Use

342.1 PURPOSE AND SCOPE

This policy describes the use of department computers, software and systems. This is in addition to the Butte County computer and internet use policies.

342.1.1 PRIVACY POLICY

Any employee utilizing any computer, electronic storage device or media, Internet service, phone service, information conduit, system or other wireless service provided 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 communication utilizing such service might otherwise have, including as to the content of any such communication. 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

The following definitions relate to terms used within this policy:

Computer System - Shall mean all computers (on-site and portable), hardware, software, and resources owned, leased, rented, or licensed by the Tulare County District Attorney Bureau of Investigations, which are provided for official use by agency employees. This shall include all access to, and use of, Internet Service Providers (ISP) or other service providers provided by or through the agency or agency funding.

Hardware - Shall include, but is not limited to, computers, computer terminals, network equipment, modems or any other tangible computer device generally understood to comprise hardware.

Software - Shall include, 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 - Shall mean any electronic document, information or data residing or located, in whole or in part, whether temporarily or permanently, on the system, including but not limited to spreadsheets, calendar entries, appointments, tasks, notes, letters, reports or messages.

342.3 SYSTEM INSPECTION OR REVIEW

An employee's supervisor 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 when 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(s) 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.

Butte County DA's Office Bureau of Investigation

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, or related to the employee's duties, an alleged or suspected violation of a department policy, or a need to perform or provide a service when the employee is unavailable.

342.4 AGENCY PROPERTY

All information, data, documents, communications, and other entries created for the department and initiated on, sent to or from, or accessed on any department computer, or through the department computer system on any other computer, whether downloaded or transferred from the original department computer, shall remain the exclusive property of the Department and shall not be available for personal or non-departmental use without the expressed authorization of an employee's supervisor.

342.5 UNAUTHORIZED USE OF 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 computer virus or malicious software infection, 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 computer. Any files or software that an employee finds necessary to upload onto a department computer or network shall be done so only with the approval of the department IT specialist and only after being properly scanned for malicious attachments. No employee shall knowingly make, acquire or use unauthorized copies of computer software not licensed to the agency while on agency premises or on an agency computer system. Such unauthorized use of software exposes the agency and involved employees to severe civil and criminal penalties.

342.6 PROHIBITED AND INAPPROPRIATE 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 departmental use and which shall not be intentionally accessed include, but are not limited to, adult forums, pornography, chat rooms and similar or related Web sites. 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, which shall be subject to audit and review by the Department without notice. No copyrighted and/or unlicensed software program files may be downloaded. Employees shall report any unauthorized access to the system or suspected intrusion from outside sources (including the Internet) to a supervisor.

342.7 PROTECTION OF AGENCY 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.