7.5 COMPUTER PROCEDURES

The first and foremost rule for using these technologies is:

Don't say, do, write, view, or acquire anything that you would not consider to be County Business; that you do not require access to for your job responsibilities; and / or that you wouldn't be concerned to have everyone in the world learn about if the electronic records were requested for disclosure.

Conduct considered as misuse / inappropriate: *The following conduct is considered as misuse or inappropriate. They include issues dealing with copyright laws, physical harm to the computer systems, accessing information that the employee does not have permission to access, connecting or using non-County owned software or equipment on the County network, harassment via the County computer system(s), invading privacy of others via the County computer system(s), using the system for personal gain, relocation of County-owned equipment or data, and transmitting offensive material via the County computer system(s).*

Copying County-owned or licensed software or data to another computer system for personal external use;
Attempting to, or modifying County-owned licensed software without approval from the IT Administrator;
Attempting to, or accessing Operating System prompts or executing Operating System commands without approval from the IT Administrator;
Attempting to, or damaging or disrupting operation of computing equipment, data communications equipment, or data communications lines;
Attempting to, or intentionally accessing or modifying data files, databases, directories, or software without proper authorization from the IT Administrator;
Using County computing resources for purposes other than those intended, including:
Allowing access by unauthorized persons
Using County resources for personal gain
Transporting computers, data, data media, programs, documentation and/or equipment to another location unless authorized by the IT Administrator;
Invading the privacy of an individual by using electronic means to ascertain confidential information;
Copying or altering another user's software or data without permission from that user;
Knowingly accepting or using software or data which has been obtained by illegal means;
Abusing or harassing another user through electronic means;
Using the County's computing facilities in the commission of a crime;
Using the County's computing resources to access, transmit, store, display or request obscene, pornographic, erotic, profane, racist, sexist or other offensive material (including messages, video, images or sound);
Connecting or attaching equipment not purchased by Sac county to County-owned workstations and equipment without approval from the IT Administrator and Department Head; and
Installing or using software not purchased by Sac county on County-owned workstations and equipment; or knowingly copying or using programs in contravention of copyright laws.
Attempting to remotely access any County system(s) using non-official means such as a backdoor or Trojan program or any other method in an attempt to circumvent the firewall and/or Internet monitoring software.

Identification & Passwords: *The County's computer systems require that each user have a unique identity, referred to as a "User-Id", protected by a "Password", to gain access to the system. This identity and password are used to represent an End User in various system activities, to provide access to certain software and data based on his/her duties and purpose for requiring such access. As such, this computer identity is another instrument of identification and its misuse constitutes forgery or misrepresentation. Conduct which involves misuse of User-ID and Password includes:*

Allowing another individual to use the identity and password;
Using another individual's computer identity and password even if the individual has neglected to safeguard his or her computer identity
If access to a system is needed and the individual is not available, the Department head will contact the IT Administrator.

Security Concerns: *The following issues deal with the security of the system and cover items concerning the location of the equipment, using equipment that is approved by the IT Administrator as well as the Department Head / Elected Official, security precautions for mobile devices in the event of (or to prevent) a loss or theft of equipment, unsafe websites and end user security training.*

The placement of a computer system in a user area and the portability of the equipment and associated data media creates special user concerns, as outlined below:

- The IT Administrator and the End Users must ensure that all equipment is located in a secure area where the opportunities for theft are minimized.
- The End User must ensure that only authorized personnel have access to the computer system and that only legitimate items of County business are processed thereon.
- Local data files must be safeguarded from unauthorized access.
- The ability to load a large amount of data on an easily transported media makes it imperative that confidential data be carefully controlled and safeguarded.
- Mobile Devices, including but not limited to: laptops, cell / smart phones, iPads, etc. that are issued by Sac county as well as personal devices (limited to cell phones / smart phones only) that are used for business purposes and / or store Sac county information shall adhere to the following guidelines:
- Access to Sac county information resources using a mobile device must be pre-approved by the IT Administrator and the Department Head / Elected Official;
- Mobile devices must require a pin / pattern / password lock to access; Mobile devices must require a pin / pattern / password lock after a period of inactivity;
- Encryption is required for all mobile devices that must store or access sensitive information. (Please contact the IT Administrator for assistance establishing data encryption);

Users that use personal mobile devices for business must follow the same guidelines as those users who are issued County-owned devices;

- Users will physically secure mobile devices that are left unattended. (If left in a vehicle, mobile devices will be hidden from view, locked in glove compartment, etc.);
- Users are not allowed to provide unattended access to mobile devices by another user;
- Users will notify the IT Administrator immediately if mobile device is lost or stolen;
- Users will return Sac county provided mobile devices at the end of employment. At which time the device will be wiped.
- Disable Bluetooth unless needed
- Personal devices, excluding cell phones / smart phones, shall not be connected to any Sac County network.

The IT Administrator shall establish security rules regarding websites deemed to be dangerous and / or inappropriate for End User access. These websites shall be blocked via hardware and software settings.

The IT Administrator shall establish periodic End User Security Training. All End Users of County Systems shall be required to attend this training and / or review the training materials provided during the training session.

Equipment Care, Maintenance, and Disposal: *This section of the policy is a general guideline for keeping County owned computer equipment safe from physical harm from outside elements.*

Users must ensure that their computers are not exposed to extremes of heat or cold, dust, smoke, or other potential contaminants. Drinks and food should be kept away from the equipment or storage media. The IT Administrator should be advised of any malfunctions arising with the equipment.

Internet access is to be used to communicate with fellow employees and clients regarding matters within an employee's assigned duties, to acquire information related to or designed to facilitate the performance of regular assigned duties, and to facilitate performance of any task or project in a manner approved by an employee's Supervisor.

No one shall use any County computer hardware, software, network facilities, or information without proper authorization. No one shall assist in, encourage, or conceal from the County any unauthorized use, or attempt at unauthorized use, of any County computer hardware, software, network facilities, or information.

Virus-checking software is made available to users of the County's network environments and should be used with all electronic files or other software loaded onto County equipment or introduced by any means (i.e., Internet, floppy disk, CD-ROM, file transfer, DVD, jump drive or other sources).

No one shall copy, install, or use any software or data files in violation of applicable copyrights or license agreements. No software shall be installed on County equipment without prior authorization of the supervisor.

End User responsibilities: Secure their account and passwords. The IT Administrator will presume that all use of the account and passwords to be by the authorized End User of that account and passwords.

End Users must:

- take reasonable precautions to prevent the account and passwords from becoming known to other persons;
- Take reasonable effort to use the Internet resources effectively, economically and responsibly;
- Advise the IT Administrator or their supervisor/manager if information to which the End User is not entitled has been inadvertently obtained or sent, or they become aware of a breach of security;

In the use of County Internet access, the following is prohibited:

- Dissemination or printing of copyrighted materials (including articles and software) in violation of copyright laws;
- Sending, receiving, printing or otherwise disseminating proprietary data, trade secrets or other confidential information, including client information, of the County in violation of policy or proprietary agreements;
- Offensive or harassing statements or language including disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religious or political beliefs;
- Sending or soliciting sexually oriented message or images;
- Operating a business, usurping business opportunities or soliciting money for personal gain, or political lobbying activities, or searching for jobs outside of the County; and,
- Sending chain letters, gambling, or engaging in any other activity in violation of local, state or federal law.

Social Media Sites: Sac county provides access to Social Networking sites including, but not limited to, *Facebook* and *Twitter*, to its employees for the sole purpose of providing access to such sites to conduct Sac county business only. These sites can be beneficial to County-related business and should be used in such a manner to promote Sac county and relay County- related Information to the public. It is the intent of this policy to ensure that users maintain discretion and professionalism while using these sites so as to not harm the reputation of Sac County.

Sac County has the right to disable commenting on any Social Media sites. It will be up to the Department Heads discretion to have commenting on or off, on their Social Media platform.

General Provisions: County Internet, E-mail, and voicemail technology are the property of Sac County. All communications and activities conducted on the County-owned systems and equipment are the property of the County. The employee should have no expectation of personal privacy when using County-owned systems or equipment. The County may review, audit, or download messages that employees send or receive and may monitor Internet access. County computer and telecommunications equipment is provided solely for business use only, and personal use is strictly prohibited.

Use of the County technology systems is a revocable privilege. Should an employee wish to clarify whether the use of any County technology is questionable, it should be discussed with the Supervisor for approval.