10.0 COUNTY COMPUTERS, CELL PHONES AND SOCIAL MEDIA POLICY

PURPOSE

The purpose of this policy is to provide instructions for agency personnel regarding the use of county owned computer equipment, software, Internet, Electronic Mail (E-Mail), cell phone and social media use.

All county owned computers, digital data devices, software and cell phones are for the official use of the Washington County Sheriff's Office and are intended to improve the efficiency and effectiveness of the Sheriff's Office operations.

Operation of all of the above equipment and programs must be in accordance with established security measures as outlined below and shall be limited by security access as determined by County Information Technology personnel and the Sheriff. Records and information maintained by the Washington County Sheriff's Office are for the exclusive use of Sheriff's Office employees only in the performance of their official duties and shall not be disseminated to persons who are not affiliated with the Sheriff's Office or as approved by the Sheriff or established by Sheriff's Office policy.

DEFINITIONS

County Owned Computer Equipment – For purposes of this order, the term "County Owned Computer Equipment" refers to:

A. All desktop and laptop computers issued or owned by the County, to include all accessories, peripherals and software.
B. All computer network equipment, routers, access points, modems, etc. that are part of Washington County's computer network system.
C. All iPads, tablets, thumb drives, portable hard drives or other digital electronic equipment issued or owned by the County.
D. Any cell phone or smart phone issued or owned by the County.
E. Any access to the Internet, World Wide Web, email, Facebook, other social media, Computer-Aided Dispatch, Records Management System, and Police Mobile software provided by the County.

Breach – A break in the system security that results in admittance of an unauthorized person or program to County Owned Computer Equipment.

Electronic Mail (E-Mail) Message – Any document created or received on the Electronic Mail System. These documents include, but are not limited to, brief notes, announcements, memorandums, and any attachments to messages, such as word processing or spread sheet documents, photographs, video, etc.

Electronic Mail (E-Mail) System – A computer application that is used to create, receive, transmit, store and archive Electronic Mail Messages.

Firewall – A form of access-control technology that prevents unauthorized access to information resources by placing a barrier between an organization's network and an unsecured network.

Hardware – The physical computer system or any physical part or mechanism used as an integral or peripheral component of a computer system (e.g., hard drive, memory, motherboard, display monitor, network cards, etc.).

Intranet – An Intranet uses Internet-based technologies within an organization to facilitate communication and provide integrated access to information.

Internet – A worldwide network of computers linked together by various communication systems including local telephone systems and fiber optic systems.

Network – A system of computers, printers and hard drives linked by direct connect, over telephone lines, or via other electronic transmission methods that allows shared access to all resources on the network.

Social Media – A category of Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social networking sites such as Facebook, MySpace; microblogging sites such as Twitter and Nixle; and photo and video sharing sites such as Flickr and YouTube.

Social Network – Online platforms where users can create profiles, sharing information, and socialize with others using a range of technologies.

Software – The programming instructions and data the computer executes to perform tasks, including the use of other media such as CD-Rom, thumb drive, etc. to distribute such software.

Speech – Expression or communication of thoughts or opinions in spoken words, in writing, by expressive conduct, symbolism, photographs, video or related forms of communication.

Virus – A self replicating computer program capable of attaching itself covertly to files. Can also be an executable program designed to perform actions not authorized by the system's user, i.e. making the system mail the virus to the first 50 people in the user's address book.

World Wide Web – A portion of the Internet that transmits information in the form of text, graphics, sound and video.

Worm – A computer program designed to covertly destroy or manipulate data, but cannot attach itself to other programs. A worm still replicates itself to other computers and uses memory, but will always arrive in the same program.

10.1 GENERAL POLICY AND ADMINISTRATIVE GUIDELINES

A. These policies apply to all members of the Washington County Sheriff's Office. Use of these County Owned Computer Equipment and Systems implies that Sheriff's Office personnel agree to comply with all applicable policies, guidelines and laws regarding their use.

B. System Administrators will be assigned the responsibility for all computer security, access and the operation of computer systems utilized by the Washington County Sheriff's Office. Each employee will use a unique password and system login as designated by the System Administrators. [CALEA 82.1.9]

C. The System Administrators shall be the only County employees authorized to issue user login and passwords and shall determine, based upon the user's duties, the level of access to computer systems. [CALEA 82.1.6]

D. The System Administrators shall be responsible for backing up computer systems daily. Other backup routines may be performed as needed. Backup media will be stored in a secure location and maintained by the System Administrators. [CALEA 82.1.8]

E. Only the Information Technology personnel, or their designee, will install hardware/software on agency computers.

F. Information Technology personnel are responsible for granting and monitoring access to Agency computer systems by issuing each Agency member a "Computer Account." A member is prohibited to use any "Computer Account" which is assigned to another person.

G. Members are responsible for their own Computer Account, regardless of who actually uses it; therefore, they are responsible for logging off the network upon completion of their computer work or upon leaving the computer for extended periods of time.

1. The use of software/hardware on agency computers will be limited to lawful and productive endeavors.
2. The unauthorized copying of computer software is prohibited.
3. Hardware and software will only be installed by Information Technology personnel or their designee.
4. When required for legal compliance, all software installed on agency computers will be registered or licensed with the software manufacturer. Registration and/or licensing information will be maintained by Information Technology personnel.

H. Members shall not disclose their login and passwords, access codes, or other authentication devices to other members, except to System Administrators who may be troubleshooting their system.

I. Unless approved by the Sheriff, the e-mail system will not be used for:

1. Disseminating confidential materials or agency sensitive information, official documents that must be retained in their physical form, or documents that require a physical signature to certify a receipt.
2. Charitable endeavors.
3. Private business activities.
4. Inappropriate entertainment purposes.
5. Other inappropriate materials or comments.
6. Members will not use obscene, racist, or sexist language in email and will not transmit threatening or harassing material (i.e., jokes, photographs, or programs forwarded as attachments), nor engage in any form of sexual harassment.
7. Every member using the email system shall check their email box at a minimum of at least once per work day to ensure timely dissemination of information.
8. Every member using the email system will be able to store a limited number of email messages within the system. If storage space becomes limited, a member will be required to remove all messages which are not required to be saved.
9. Email messages sent or received by agency members are not private and the agency reserves the right to monitor all email messages without notification to the member. However, it is not the agency's intent to monitor all email messages. It is a violation of this policy for any user, including system administrators to access the email system or messages of others simply to satisfy curiosity about the affairs of others.
10. Every email message should be both professional and courteous.

J. Users may not alter or copy a file belonging to another user without first obtaining the permission from the owner of the file. The ability to read, alter or copy a file belonging to another user does not imply permission to read, alter or copy the file.

K. Users may not use Agency computer systems to invade the privacy of other agency members by unnecessarily reviewing their files or email.

L. Members will not use the agency computer system to harass, make defamatory remarks toward others, or perform illegal malicious acts.

M. Members will not interfere with or disrupt any County computer system, Internet user, program or equipment. Disruptions include, but are not limited to, propagation of computer worms, viruses, or other debilitating programs, and using county computer systems to make unauthorized entry to any other machine accessible via the computer system or Internet.

N. Viruses can cause substantial damage to the County computer systems. Each user is responsible for taking reasonable precautions to avoid introducing viruses to the County computer systems.

1. Files obtained from any source outside the agency, including computers or other media brought from home; files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to e-mail; and files provided by vendors, may contain dangerous viruses.

2. Users should never use media sources from non-agency sources or download Internet files or accept e-mail attachments from unknown sources without first scanning the material with agency installed anti-virus software. If a user suspects that a virus has been introduced into the county computer network, he/she shall notify the Information Technology personnel immediately.

O. Members who become aware of any computer system security breach, whether internal or external, will immediately notify the Information Technology personnel.

P. Any member observing someone using the agency computer system inappropriately will notify his/her supervisor. The supervisor receiving such information will take the appropriate action.

Q. Members with proper authorization by the Sheriff may utilize privately owned computers for agency business.

1. Privately owned computers will only connect through the County computer system through authorized connections via the Internet as approved by the Sheriff and established by Information Technology personnel.
2. Members will be responsible for and adhere to agency computer policies when utilizing privately owned computers for agency business or connected to County computer systems.
3. Personal hardware components, such as printers, external modems, external hard drives, thumb drives, CD-Rom, etc., will not be connected to Agency computers.
4. Technical support on privately owned computers for agency business will be considered on a case by case basis and approved by the Sheriff.

R. Those employees who have State and National computer system security shall access those files and records in accordance with specific training provided for the use of the State or National computer systems. Members will not violate the guidelines for access provided for accessing the State or National computer systems.

S. Information retrieved from State and National computer files and the National Law Enforcement Telecommunications Network (N.L.E.T.S.) is intended for official police use only and the dissemination of this information to non-criminal justice individuals is strictly prohibited and could subject the offender to criminal and civil penalties [§ 12-12-212]. [CALEA 82.1.1d]

T. Any employee who disseminates Criminal History information from any State or National computer system must log that dissemination into a Criminal History log which shall be maintained within areas where State and National Criminal History information may be gained. [CALEA 82.1.9]

U. Dissemination of Criminal History information as described above must be to Criminal Justice officials, outside the Sheriff's Office agency, authorized to receive Criminal History information. [CALEA 82.1.9]

V. The Criminal Justice official receiving the information must be identified by Organization, name, employee number or social security number, address and phone number along with the date and time the information was disseminated. [CALEA 82.1.9]

W. Members authorized to use Social Media representing the Washington County Sheriff's Office shall do the following:

1. Conduct themselves at all times as representatives of the agency and shall adhere to all agency standards of conduct and observe conventionally accepted protocols;
2. Identify themselves as member of the agency;
3. Not make statements about the guilt or innocence of any suspect or arrestee, or comments concerning pending prosecutions, nor post, transmit, or otherwise disseminate confidential information, including photographs or videos, related to agency training, activities, or work related assignments without the approval of the Sheriff;
4. Not conduct political activity or private business; and
5. Observe and abide by all copyright, trademark, and service mark restrictions in posting materials to electronic media.
6. The use of agency computers by agency members to access social media is prohibited without prior approval by the Sheriff. Members shall not access social media for personal use while on duty, unless approved by a supervisor for purposes of conducting an investigation.
7. Any employee who maintains a blog, or who reply to blogs that identify the agency must identify themselves, and include a disclaimer that their viewpoints are personal, private, and do not necessarily reflect the position of the agency.
8. Employees having a work-related complaint(s) shall notify their supervisor, in an effort to resolve the complaint, prior to blogging or posting about complaint(s).
9. Employees shall not knowingly or recklessly post false information about the agency, supervisors, coworkers, public officials, and others who have a relationship to or with the agency, to include wrongful disparagement of fictitious characters that resemble known personnel or officials.

X. Members shall abide by the following when using social media for personal use while off-duty:

1. Members are free to express themselves as private citizens on social media sites to the extent that their speech does not impair working relationships of this agency for which loyalty and confidentiality are important; impede the performance of duties; impair discipline and harmony among coworkers; or negatively affect the public perception of the agency;
2. As public employees, agency members are cautioned that while on or off-duty, speech made pursuant to their official duties is not protected under the First Amendment and may form the basis for discipline if deemed

detrimental to the agency. Members should assume that their speech and related activity on social media sites will reflect upon their office and this agency;

3. Members shall not post, transmit, or otherwise disseminate any information obtained as a result of their employment with the Washington County Sheriff's Office without written permission from the Sheriff;
4. For safety and security reasons, members are cautioned not to disclose their employment with this agency and shall not post information pertaining to the employment of any other member without prior consent by that member. As such, members are advised to use good judgment when placing or allowing photographs or depictions of themselves dressed in Washington County Sheriff's Office uniform and/or displaying official identification, patches or badges, or in any other way, either directly or indirectly, identifying themselves as a member of the agency for any reason.

Y. Without prior approval by the Sheriff, members shall not post, transmit and/or disseminate photographs or other depictions of agency uniforms, badges, patches, issued equipment, or marked/unmarked vehicles, photographs of the inside or outside of Sheriff's Office buildings or facilities, courtrooms, crime scene or accident scene photographs, agency photographs, video or comments on agency training, activities, investigations, or other work related assignments or information on Internet sites.

Z. Members are reminded that their speech on social media becomes part of the World Wide Web electronic domain. Therefore, members shall adhere to the Code of Conduct of the Washington County Sheriff's Office when using social media for personal or business use.

AA. Members shall not post sexual, violent, racial, ethnically derogatory material, comments, photographs, artwork, video or other references along with any agency approved reference.

BB. Members issued cell phones or smart phones by the agency shall limit the use of the phone to agency business. A limited number of personal calls may be made in cases of emergency but the member must stay within the limitations of their calling plan.

CC. All of the policies pertaining to computer use, security, social media, etc. shall also apply to the use of their assigned cell phone or smart phone.

DD. Any violation of this policy and/or misuse of electronic media will result in disciplinary action, including termination of employment.

EE. Any exception to the agency's electronic media policies must be approved, in writing, by the Sheriff.