

4.01
CRAIG POLICE DEPARTMENT
Office of Chief of Police
General Order

Date Issued: February 11, 1999

Revision Date: April 1, 2009

Subject: Information Systems Use Reference: CACP STD.

TO: ALL OFFICERS

I. POLICY

The availability and use of the personal computer within the work environment have provided many opportunities for enhancement of productivity and effectiveness. These technologies also entail the opportunity for rapid transfer and broad distribution of sensitive information that can also have damaging effects on this department, its members, and the public if not managed properly. Therefore, it is the policy of this department that all members abide by the guidelines set forth herein when using personal computers and the services of both internal and external databases and information exchange networks, and where applicable, voice mail, mobile digital terminals, and related electronic messaging devices. Communications sent by e-mail may be subject to disclosure under the Public Records Act (C.R.S. 24-72-203) or in litigation. No employee shall have any expectation of privacy with regards to any information on the computer systems.

II. PURPOSE

It is the purpose of this policy to provide employees with guidance on the proper use of personal computers and related electronic messaging systems utilized in this department for purposes of disseminating electronic mail, utilizing services of the Internet and related electronic message transmission, recording and storage devices.

III. DEFINITIONS

Information Systems (IS): For purposes of this order, information systems include personal computers, electronic mail systems, voice mail systems, paging systems, electronic bulletin boards and Internet services, mobile digital terminals, and facsimile transmissions.

NCIC/CCIC: the National Crime Information Center and the Colorado Crime Information Center are computer systems managed by the Colorado Bureau of Investigation for criminal investigation purposes, as well as an integral and important responsibility of department members authorized to utilize the system. Any misuse of this system could result in criminal prosecution and/or suspension of authorization to operate within the system and disciplinary action up to and including termination.

IV. GENERAL PROCEDURES

- A. Transmission of electronic messages and information on communications media provided for members of this department shall be treated with the same degree of propriety, professionalism, and confidentiality as official written correspondence or public records.
 - 1. This includes all cell phone call history, text messaging, etc.

- B. This department encourages authorized and trained personnel with access to IS to utilize these devices whenever necessary. However, all these devices are the property of the City of Craig and use of any of these devices is a privilege that is subject to revocation.
- C. IS and their contents are the property of this department and intended for use in conducting official business with limited exceptions noted elsewhere in this order.
- D. Members are advised that they do not maintain any right to privacy in IS equipment or its contents, to include personally owned software (if approved).
 - 1. The department reserves the right to access any of the records within the system at any time and to retain or dispose of those records as it deems necessary and appropriate, and may require members to provide passwords to files that have been encrypted or password protected.
 - 2. The department reserves the right to access, for quality control purposes and/or for violations of this policy, data, electronic and voice transmissions of members conducting business of this department.
- E. Accessing or transmitting materials (other than that required for police business) that involves the use of obscene language, images, sexually explicit materials, or messages that disparage the department, any person, group, or classification of individuals is prohibited whether or not a recipient has consented to or requested such material.

Exception: Officers involved in criminal investigations that involve computer crime(s) may be required to receive, copy or download sexually explicit material.
- F. Confidential, proprietary, or sensitive information may be disseminated (or made available through shared directories or networked systems) only to individuals with a need and a right to know and when there is sufficient assurance that appropriate security of such information will be maintained. Such information includes but is not limited to the following:
 - 1. Transmittal of personnel information, such as salary, performance reviews, complaints, grievances, misconduct, disciplinary information, medical records, or related employee information.
 - 2. Criminal history information and confidential informant master files, identification files, or related information.
 - 3. Intelligence files and information containing sensitive tactical and undercover information.
- G. No member shall access or allow others to access any file or database unless that person has a need and a right to such information. Additionally, personal identification and access codes shall not be revealed to any unauthorized source.
- H. An IS is designed and intended to conduct business of this department and is restricted to that purpose. Installation of or access to software for purely entertainment purposes is

prohibited without the approval of the Chief of Police. Exceptions to business use include the following:

1. Infrequent personal use of these devices may be permissible if limited in scope and frequency. The use must be in conformance with other elements of this order, and not connected with a profit-making business enterprise or the promotion of any product, service, or cause that has not received prior approval of this agency.
2. Personnel may make off-duty personal use of agency computers for professional and career development purposes when in keeping with other provisions of this policy and with prior knowledge of an appropriate supervisor.

I. Any electronic mail (e-mail) sent outside of the department network must contain the following disclaimer placed at the bottom of the message:

*****“This e-mail and any files transmitted with it are the property of the Craig Police Department, are confidential, and are intended solely for the use of the individual or entity to which it is addressed. If you are not the intended recipient (or responsible for the delivery of the message to the intended recipient), you are hereby notified that any dissemination, distribution, copying, or other use of, or taking of any action in reliance on this e-mail is strictly prohibited, and may be unlawful. If you are not one of the named recipient(s), or otherwise have reason to believe that you have received this message in error, please notify the sender at (970) 826-2360 and immediately delete this message and all attachments from your computer.”

J. NCIC/CCIC

1. All authorized personnel will receive training on the system, where additional resource materials are kept and in the procedures for trouble shooting problems. They will also be familiar with information contained in the NCIC Operating manual.
2. All authorized personnel will be familiar with the CCIC procedures and release of information requirements.
3. Warrants: Any Municipal Court warrants will be entered into the CCIC system by the appointed person and filed accordingly. CICJIS will control any other warrants.
4. The CCIC Newsletter is available on the 15th of each month. Each CCIC operator is responsible for accessing and reviewing it on a monthly basis.
5. Switched Messages: Switched messages pertinent to our area shall be printed and placed on the clipboard in the patrol area where they are available to all law enforcement personnel. Messages pertaining to training, equipment, or other items of interest shall be printed and placed in the distribution box of the person having an interest in that particular item.

6. Access to the CBI computer system (NCIC/CCIC) is only allowed from computers located in the Public Safety Center, or those approved by a supervisor for a law enforcement branch location. Each operator is expected to abide by the rules and regulations set forth by NCIC/CCIC policies.
 - a. All operators are required to test every two years to maintain their OSN status.
7. The public may be given the website address for CBI to obtain information available to the public.
8. Information retrieved from NCIC/CCIC system is confidential and shall not be disseminated to the public.

V. IMPORTING/DOWNLOADING INFORMATION AND SOFTWARE

- A. Members shall not download or install on their personal computer or network terminal any software, or other materials from the Internet or other external sources without taking prescribed steps to preclude infection by computer viruses.
 1. Material shall be downloaded to storage devices (CD's thumb drives, etc.) and scanned for viruses prior to being entered into any personal or shared system.
 2. In no case shall external materials or applications be downloaded directly to any shared (network) drive. When in doubt, members shall consult the system manager for guidance.
- B. Members shall observe the copyright and licensing restrictions of all software applications and shall not copy software from internal or external sources unless legally authorized.
 1. Any software for which proof of licensing (original disks, original manuals and/or license) cannot be provided is subject to removal by authorized agency personnel.
 2. Privately owned software may not be loaded on agency computers without approval of the system administrator or Chief of Police.
- C. Members shall observe copyright restrictions of any documents, images, or sounds sent through or stored on electronic mail.
- D. Any hardware enhancements or additions to agency-owned equipment must be approved and authorized by the designated system administrator and Chief of Police. The system administrator is responsible for determining proper installation procedures.
- E. Members shall not permit unauthorized persons to use this agency's Records Management, electronic mail or other computer systems.
- F. To avoid breaches of security, members should log off any personal computer that has access to the agency's computer network, electronic mail system, the Internet, or sensitive information whenever they leave their workstation.

G. Any misuse of the IS may result in disciplinary action and/or termination.

VI. INTERNET INFORMATION CONCERNING THE DEPARTMENT

A. Creating a web site on the Internet that has any appearance of officially representing the City of Craig, or the Craig Police Department is prohibited without the express approval of the Chief of Police.

1. Any official department web pages or sites will be at the direction of the Chief of Police and must have his/her approval prior to being accessible to the general public.

B. Using scanned images of any official department logo; patch or badge on personal web pages is prohibited without the express written approval of the Chief of Police.

Approved by:



Walter K. Vanatta
Chief of Police