I. POLICY

The Department’s various computer systems are designed to increase the work performance and efficiency of all members. The computer’s main virtues are rapid transmission of communications and storage and retrieval of massive amounts of information.

The operation of any Department computer system must never be used in such a manner as to violate any law, regulation, policy, or directive. In addition, use of the computer system is primarily restricted to tasks and efforts related to the operation of the Davis Police Department and/or the City of Davis.

Current law holds that users of employer computers while engaged in the scope and course of their employment have no expectation of privacy in the use of any computer system or email, provided the employer declares that inspection or surveillance of its computers may occur. By this order, the Police Department declares that no such expectation of privacy exists, except where specifically identified.

All e-mail messages, including attachments, transmitted over the Department computer network are considered Department records and, therefore, are the property of the Department. The Department reserves the right to access, audit, and disclose for whatever reason, all messages, including attachments, transmitted over its e-mail system or placed into its storage.

The e-mail system is not a confidential system since all communications transmitted on, to or from the system are the property of the Department. Therefore, the e-mail system is not appropriate for confidential communications. If a communication must be private, an alternative method to communicate the message should be used instead of e-mail. Members using the Department’s e-mail system shall have no expectation of privacy concerning communications utilizing the system.

Members are provided with login identification (ID) for various department computer systems. Members must maintain the privacy of their login ID and password. Members are not permitted to share passwords with others.
II. PROCEDURE

A. Computer Audit or Inspection

1. There is no expectation of privacy in a member’s private filing area on the network server or in the cities email system (Includes City Network, Outlook, and any other private filing area or E-mail system stored or accessed on any department system).
   
a. Entry into a private filing area or the email system may occur in response to a lawful subpoena, court order, or with the specific authorization of a member of the Executive Staff for either specific or audit purposes.

b. Consistent with normal police investigative practices, members will normally be advised in writing whenever their files are examined or audited. Such notification may be delayed until the completion of a criminal or internal affairs investigation.

2. DPOA Filing Area
   
a. Entry into the DPOA Filing Area is prohibited except to authorized users. Any other entry shall only be in response to a subpoena or court order.

3. Mobile Data Computer Transmissions
   
a. There is no expectation of privacy regarding any MDC transmission. The Police Department will routinely audit the records of MDC transmissions to ensure transmissions are in compliance with the provisions of Section I, above.

B. Mobile Data Computers

1. Authorized Use of Equipment
   
a. Members will not use the MDC equipment unless they have successfully completed training in its use.

2. Dispatch Procedures
   
a. Calls will be broadcast via voice-radio pursuant to current dispatching procedures. Calls should be sent to the MDC for reference and possible disposition via the MDC.

b. If MDC dispatching is more appropriate for a specific event requiring confidentiality or which is on a need-to-know basis (e.g., stolen police vehicle or a scanner is suspected), a supervisor may approve dispatching the event via the MDC alone.

c. A supervisor may approve MDC dispatching for low risk/priority calls during periods where there is a high volume of calls.

3. Stolen Vehicle/Wanted Persons Hits
   
a. If a field unit runs a vehicle plate via the MDC and it returns as a reported stolen vehicle, the officer will immediately notify dispatch. The dispatcher will confirm the status of the return.

b. If a field unit inquiry reveals a subject is possibly wanted, the unit shall immediately notify dispatch of the possible hit and request that it be confirmed.
4. Cancellations
   a. Any cancellation of a unit response by dispatch shall be broadcast and acknowledged verbally.
   b. Field units shall be responsible for a verbal broadcast of situation secure (Code 4) and/or the cancellation of other units responding when no further assistance is needed.
   c. When preempting a unit from a current assignment, the dispatcher shall verbally broadcast the cancellation of the first call prior to assigning the new call.

5. Address and Premise History
   a. Officer safety information pertinent to the call an officer is enroute to shall be provided via voice broadcast and acknowledged verbally by the officer.
   b. Premise information provided by CAD may be sent to the unit via the MDC.

6. E-Mail and Chat
   a. The MDC has message sending capabilities generally referred to as E-mail and Chat.
   b. E-mail and Chat should not be used for call updates, supplements or dispatch requests. Dispatch will not be responsible for monitoring these features, unless requested by a supervisor.

7. Log Off
   a. Field units shall advise dispatch when they go off-duty (10-10) via radio broadcast at end of watch.
   b. It is the field units’ responsibility to properly log off the MDC at the end-of-watch.
   c. The MDC shall not be logged off or turned off during the shift, except as authorized.

8. Use While Driving
   a. Members should use reasonable caution in the operation of the MDC while driving. Extensive reading and typing should not be done while driving. While the car is in motion, driving takes precedence over other tasks.

9. Non-Operational Units
   a. If a system is found to be non-operational after conducting standard troubleshooting procedures outlined in training, the member shall report this to their supervisor and to the E-Mail group PD IS.
   b. Vehicles may not be placed out of service solely on the non-operational condition of the MDC.
C. Prohibited Conduct

1. Prohibited Acts

   a. Members are prohibited from logging into any computer with another persons login ID or transmitting messages in the computer system representing themselves as another person.

   b. Members are prohibited from transmitting messages in the computer system which are: defamatory; threatening; racially, ethnically, or sexually offensive; or which are regarding religious or political activities, including DPOA activities relating to other than planned events or meetings or announcements; copyright infringement; personal gain; solicitation; or in support of illegal activities. Other prohibited uses include but are not limited to: transmitting sexual remarks or offensive jokes, profanity, and all jokes or off-color remarks relating to the use of force, citizen contacts, and/or dispositions of calls.

   c. E-mail messages addressed to the entire department are only to be used for official business related items that are of particular interest to all users.

   d. Except when necessary, and in conjunction with a criminal investigation, and with the approval of the Investigations Division Commander, members are prohibited from transmitting, receiving, storing, or seeking sexually explicit material in e-mail, private filing areas, over the internet, or through any other electronic means.

2. Violations of Policy

   a. Members identified as being responsible for violations of this policy will be subject to corrective training and/or discipline.

Darren Pytel
Police Chief
2/97

Rev. 9/99,
2/00,
10/02 MDC policy added
1/04 additions to c,1,b
3/07 Policy updated for RIMS changes
03/10, update to email communications clarifying there is no expectation of privacy
5/19

Reviewed 12/00, 1/02, 1/03, 1/04, 9/05, 10/07, 12/09, 10/11, 03/16, 12/17
Davis Police Department

EMPLOYEE STATEMENT FORM
USE OF POLICE INFORMATION SYSTEMS

As a Member of the Davis Police Department you have access to information systems such as RIMS, CAD, CLETS/NCIC, etc. Department and CLETS Policy sets forth rules for both use and dissemination of information derived from these sources.

Members are advised that e-mail, chat and other forms of communication via the computer, internet, and/or radio are subject to administrative auditing to ensure compliance with policy.

Member Acknowledges that:

- The use of computer systems shall be restricted to official business only.
- Records of all messages, Internet use, chat, etc. are generally held to be public records and are subject to review and release by the media.
- Inappropriate or unprofessional messages shall not be transmitted.
- Accessing any system to gain unauthorized access to another person’s e-mail, voice mail, etc. is prohibited.

Member Statement:

I have read the above and understand the policies regarding the proper use of Information Systems.

Name: ________________________________
Signature: ____________________________
Date: ________________________________

Div Mgr: ______________________________