OFFICE OF CHIEF OF POLICE
OAKLAND POLICE DEPARTMENT

MEMORANDUM

TO: All Personnel DATE: 1 Jul 09

SUBJECT: Revision of Departmental General Order I-1, PERSONAL COMPUTERS AND ELECTRONIC MESSAGING DEVICES (Rev. 6 Feb 01)

The subject order has been revised to update Departmental policy and procedures regarding standards governing the use of Department-issued electronic messaging devices utilized for the purpose of composing and disseminating electronic mail, accessing the Internet and related electronic transmissions, and the recording, storage, and synchronous transfer of electronic data.

Additionally, this order applies to privately-owned electronic messaging devices used for transmitting or receiving Department and non-Department related business.

The provisions of Chief of Police Memorandum dated 12 Sep 01 has been incorporated into this order and is hereby canceled.

The Evaluation Coordinator for this order shall be the Personnel, Training, Technology Division Commander, who, without further notice, shall forward the required report to the Chief of Police on or by 4 Jan 10.

The Evaluation Coordinator shall receive, review and document the acceptance or rejection of all comments and/or recommendations received prior to submitting his/her six-month evaluation report.

The Evaluation Coordinator shall forward a copy of the six-month evaluation report, along with the comments/recommendations received, to the Office of Inspector General to be maintained in the appropriate Departmental General Order archive folder.

Personnel shall acknowledge receipt, review, and understanding of this directive in accordance with the provisions of DGO A-1, DEPARTMENTAL PUBLICATIONS.

By order of

Howard A. Jordan
Acting Chief of Police

Date Signed: 7/1/09

DEPARTMENTAL
GENERAL
ORDER

I-1

Index as:

Computers, Personal and
Electronic Messaging Devices

Effective Date:
1 Jul 09

Evaluation Coordinator:
PTT Division Commander

Evaluation Due Date:
4 Jan 10

Automatic Revision Cycle:
3 Years

PERSONAL COMPUTERS AND ELECTRONIC MESSAGING DEVICES

The purpose of this order is to set forth Departmental policy, procedures, and standards governing the use of Department-issued electronic messaging devices utilized for the purpose of composing and disseminating electronic mail, accessing the Internet and related electronic transmissions, and the recording, storage, and synchronous transfer of electronic data.

Additionally, this order applies to privately-owned electronic messaging devices used for transmitting or receiving Department-related business.

For purposes of this order, Electronic Messaging Devices (EMD) include personal desktop and mobile (laptop) computers, printers, monitors, cellular phones, and telecommunications devices [e.g., personal data assistant (PDA), electronic mail (e-mail) systems, voice mail systems, paging systems, electronic bulletin boards and Internet services, and facsimile transmissions].

Electronic communications and information storage (letters and paper files), are a common part of daily police activities and, therefore, part of the legal environment. As such, electronic communications are discoverable and are routinely subpoenaed and used as evidence in court. Current electronic audit techniques allow resurrection of almost all electronically sent messages.

This policy shall serve two primary goals:

1. Protect the rights of the member or employee to privacy.
2. Protect the Department from abusive use of these electronic systems.

I. POLICY

A. All Department personnel shall abide by the guidelines set forth herein when using EMDs and the services of internal and external databases, information exchange networks, and, where applicable, voice mail, and mobile laptop computers.

B. Departmental personnel shall also abide by the guidelines contained in applicable City of Oakland Administrative Instructions (AI), listed in Part VI of this order.

C. Departmental personnel shall use Department-issued EMD in an appropriate and responsible manner. Personnel shall use the Internet for purposes that support the Department's mission.

D. Personnel shall check their Departmental email at least once every day during their regularly scheduled workday. Supervisors shall be responsible for ensuring this standard is observed.

E. Personnel shall obtain approval for Department-wide distribution[1] of electronic messaging from his/her Division Commander/Manager or designee prior to transmitting. The approving authority shall be identified within the email text.

F. Personnel shall use only temperate and appropriate language. Profane, obscene, offensive or inflammatory language, images, jokes, or messages that disparage any person, group, or classification of individuals is prohibited whether or not a recipient has consented to or requested such material. In the event personnel receive threatening or unwelcome communications involving Department personnel through any EMD shall make the proper notification in accordance with DGO M-3.

G. All information transmitted through an EMD shall conform to Departmental standards in accordance with the provisions of the *Manual of Rules* Sections 314.00, Professional Conduct and Responsibilities, Departmental directives, and City Administrative Instructions.

[1] For the purpose of this order, "Department-wide" includes any email distribution list beginning with "DL-***" where *** indicates any group or sub-group of personnel.

H. Accessing or transmitting pornographic or offensive materials is prohibited, except for specific police investigative purposes. Such investigative purposes shall require the prior authorization of first-level commander.

I. Department-issued EMDs and their contents are the property of the Department and are assigned to an organizational unit or individual and designated to a specific port within that unit. An EMD may be relocated within a unit or to another organizational unit with prior approval and configuration by the City Department of Information Technology. An EMD is intended for official Departmental business and is restricted to that purpose. Exceptions to business use include the following:

1. Personal use of these devises may be permissible if limited in scope and frequency, if in conformance with other elements of this policy.

2. Personnel may make limited, off-duty personal use of agency computers for professional and career development purposes when in keeping with the other provisions of this order (e.g., academic or training courses via the Internet).

3. EMDs may be utilized to record and store personal appointments, addresses, and memos in accordance with the provisions of this order.

J. Personal use of EMDs for a profit-making business enterprise or the promotion of any product, service, or cause is prohibited without prior approval by the Chief of Police.

II. SECURITY

A. All commanders/managers shall ensure all subordinate personnel are familiar with the provisions of Departmental General Order (DGO) M-9, RELEASE OF RECORDS and M-9.1, PUBLIC RECORDS ACCESS. The transmission of information by electronic means shall be treated with the same degree of propriety, professionalism, and confidentiality as official written correspondence.

B. Electronic storing, copying, scanning, transferring, printing, and/or deleting of personnel or criminal incident data from any Department source using any form of electronic media, by any form of transmission, is prohibited unless:

1. The responsible commander/manager has given prior authorization;

2. The member or employee is aware of the potential hazards and consequences of retaining data on computer equipment or media outside the Department, and

3. The member or employee is aware that data, subject to release restrictions set forth in DGO M-9 and M-9.1, cannot be viewed, used, or altered by non-Departmental persons while the data is outside the Department.

C. Members and employees do not maintain any right to privacy in Department-issued EMD equipment or its contents.

1. The Department reserves the right to access and inspect any information contained in a Department-issued EMD and supervisory personnel may require employees to provide passwords to files that have been encrypted or password protected.

2. Members and employees are on notice that the Department may search personal EMD records, bills, and text messages for the time the member is on-duty or engaged in work-related communications. Such searches shall be made only when there are reasonable grounds for suspecting that the search will reveal the employee is guilty of work-related misconduct in accordance with prevailing law.

D. No member or employee shall access or allow access to any electronic data without a need and the right to such information. Members and employees who have been issued passwords shall not share them and shall not leave them where they can be found by others.

E. Unit commanders/managers shall ensure that:

1. Members and employees in the unit understand and practice password security.

2. Computer locking keys, electronic media, and portable hardware storage devices are kept in a secure place.

3. Licensed and copyright software and documentation are not duplicated. Illegally copied software and documentation are not used on Departmental computers.

4. Members and employees observe the copyright restrictions on any documents, images, or sounds sent through or stored on any EMD.

F. To avoid breaches of security, personnel shall log off any computer that has access to any computer network, electronic mail system, or sensitive information when leaving the workstation.

III. ACQUISITION OF COMPUTER HARDWARE, SOFTWARE, AND PERIPHERALS

A. The selection of computer hardware, software and peripherals is subject to City standards. To the extent possible, the Department shall obtain standard equipment and software.

B. The Department of Information Technology (DIT) provides an online pricing guide for computer hardware, software licensing, and peripherals meeting City standards.

C. Software products purchased from outside vendors are licensed and may not be duplicated except as specified by the manufacturer.

D. Department-issued EMDs and their contents are the property of the Department and are intended for use in conducting official business with limited exceptions as noted elsewhere in this policy.

IV. DATA BACKUP

Each unit commander/manager shall ensure that members and employees employ good computer practices and perform computer data backups on a regular basis on separate storage device/media.

V. LOST, STOLEN AND DAMAGED EMDs

All personnel shall report loss, theft, or damage on an assigned EMD to their supervisor in accordance with the provisions of Departmental General Order N-5, LOST, STOLEN, DAMAGED CITY PROPERTY.

VI. REFERENCES

AI 132	**Information Technology and Resources Roles and Responsibilities**, dated August 1, 1990
AI 133	**Information Technology and Resource Standards and Guidelines**, dated August 1, 1990
AI 134	**Telecommunications Roles and Responsibilities**, dated December 31, 1990
AI 135	**Information Access Policy for CityNet**, dated July 15, 1991
AI 136	**Office Automation Hardware and Software Standards**, dated September 3, 1991
AI 140	**Electronic Media Policy, dated April 12, 2007**

By order of

Howard A. Jordan
Acting Chief of Police

Date Signed: 7/1/09