SPECIAL ORDER

DISTRICT OF COLUMBIA

Title:
Internet Use by MPD Employees

Topic/Number
SO- 01- 03

Effective Date	Distribution
January 12, 2001	**B**

Rescinds General/Special Order

I. Background

The purpose of this order is to set forth the Metropolitan Police Department's (MPD) guidelines for managing use of the Internet by its sworn and civilian members. Internet usage by MPD employees is permitted and encouraged for business purposes in supporting the goals and objectives of the Department and shall be used consistently with the policies set forth in this order.

II. Policy

The policy of the Metropolitan Police Department is that members will utilize the Internet to support and enhance the mission of the Department. Further, the Internet may be used to conduct research on crime trends, police operations, and numerous work-related topics.

III. Definitions

When used in this directive, the following terms shall have the meanings designated:

A. Downloading – the process of copying a file from the computer to the C: drive, a floppy disk, or a network drive/fileserver.

B. Electronic mail (E-mail) – the exchange of messages via transmission by computer.

C. Internet (Net) – a worldwide system of computers that have the ability to communicate and exchange information with each other.

D. World Wide Web – the collection of computers on the Internet running HTTP (Hypertext Transfer Protocol) servers. The Web allows for text and graphics to have hyperlinks connecting users to other servers.

E. Sexually Explicit – a clear expression of sex, sexes, or the sex organs.

F. Obscene – an appeal to a prurient interest in sex; utterly no redeeming social value; and a violation of contemporary national community standard.

III. Regulations

A. Internet use is restricted to the following official, job related purposes only**:**

1. Exchanging electronic mail (e-mail) with other members of the Department, community members, or other agency partners about public safety and work related issues.

2. Participating in discussions with other groups or individuals via bulletin boards with approval from the unit's commanding officer or director.

3. Performing various forms of work related research.

4. Performing word or phrase searches to locate documents through the World Wide Web.

5. Utilizing World Wide Web documents to obtain information about commercial products and/or services.

6. Use of any of the above listed functions as a means of training other employees on use of the Internet.

7. Investigating internet related crime, when assigned or authorized by a supervisor.

8. Gathering intelligence information that will assist in achieving the goals and mission of the Department.

B. Members are prohibited from using the Internet in the following manner:

1. Pursuing private commercial business activities or profit-making ventures (i.e., members/employees may not operate a business using Department computers and/or Department provided Internet access).

2. Engaging in activities of any kind for personal financial gain or other non-work related benefit.

3. Receiving or transmitting any files in violation of licensing and/or copyright restrictions.

4. Engaging in matters directed toward the success or failure of a political party/candidate for partisan political office of partisan political group.

5. Engaging in unauthorized fund-raising.

6. Using any Internet site resulting in additional costs to the Department.

7. Engaging in any prohibited discriminatory conduct or conduct which could be construed as contributing to a sexually hostile environment.

8. Obtaining or viewing sexually explicit material (except in those circumstances in which authorized members are investigating internet related crimes).

9. Engaging in activities that violate the privacy of other users.

10. Engaging in conduct meant to purposely or which could misrepresent the identity of the user (except in those circumstances in which authorized members are investigating internet related crime).

11. Sending or receiving any material that is obscene or defamatory, or which is intended to annoy, harass or intimidate another person (except in those circumstances in which authorized members are investigating internet related crime).

12. Sending and receiving unusually large e-mails or attachments; creating, sending or forwarding electronic chain letters and net surfing to accumulate points for free goods or services.

13. Creating newsgroups or discussion groups without written authorization from the Information Technology Division, Chief Information Officer.

14. Posting unofficial or preliminary crime data or otherwise disseminating information that is official Department data without proper authorization from the Director or Commanding Officer of the member's unit and, in the case of crime data, the Senior Executive Director of Organizational Development or a designee.

15. Transmitting sensitive or restricted information (i.e., criminal history information).

16. Engaging in any activity that places the Department's computers at risk of contracting viruses or becoming damaged.

17. Engaging in activities that would tend to bring discredit on the Department or activities in violation of the D.C. Code, Federal Statutes or the Department's General Orders.

V. Procedural Guidelines

A. The Information Technology Division, Chief Information Officer shall be responsible for:

1. Facilitating specific user accounts and specific computers to conduct investigative activities on the Internet as authorized by the Executive Assistant Chief.

2. Ensuring that adequate computers are equipped with software at each unit within the Department where Internet access is available.

3. Recording and monitoring use of the Internet and electronic mail by Department personnel.

4. Providing each unit Commander/Director with a monthly report that lists each site visited and the amount of time that personnel were connected to the Internet.

5. Implementing and coordinating Internet availability throughout the Department.

B. The Commanding Officer or Director shall be responsible for:

1. Informing the Chief Information Officer of the need to investigative account status; the duration of the status; the username of the user(s) who will be involved; and, the Internet Protocol (IP) address of the computer that will be used to conduct the investigation(s).

2. Ensuring that subordinates within their unit/division adhere to the Department's established guidelines and understand that failure to adhere may subject them to disciplinary action when using the Internet.

3. Determining whether a case of Internet misuse is minor or serious. Investigating all cases of Internet misuse determined to be minor and forwarding all serious cases to the Office of Professional Responsibility for it to investigate. In all cases of internet misuse, whether determined to be minor or serious, the Office of Professional Responsibility is to be notified.

// SIGNED//
Charles H. Ramsey
Chief of Police

CHR:NMJ:sg:uk