# PHILADELPHIA POLICE DEPARTMENT DIRECTIVE 7.12

| Issued Date: 02-21-92 | Effective Date: 02-21-92 | Updated Date: |
|---|---|---|

## SUBJECT: PERSONAL COMPUTERS

## 1. POLICY

A. Commanding officers are urged to encourage creativity among personnel of their units assigned to use personal computers provided such efforts do not exceed the parameters of this directive or hinder the function of their units.

B. Department personnel are required to become familiar with and adhere to all federal, state, local and copyright laws addressing automated information systems, computers, computerized files and reproduction of software or data.

C. No one will release computerized data to any outside agency without the approval of the Police Commissioner.

D. All computers and software in police installations are subject to inspection by the Standards and Accountability.

## 2. DISTRICT AND UNIT RESPONSIBILITIES

A. Commanding Officer's Responsibilities

1. Commanding Officers of units utilizing personal computers will appoint an individual (sworn or civilian) to oversee daily use of the unit's computers who will be referred to as the computer coordinator. In addition, Commanding Officers will ensure that a second individual is capable of replacing the coordinator when he/she is not available. Personnel will not be designated as computer coordinators until they have been trained or evaluated by the Advanced Training Unit (ATU).

2. Submit, when necessary, a memorandum to the Commanding Officer, ATU, listing the name, rank and payroll number of all personnel that require training or evaluation. Specify if training or evaluation is required.

3. Ensure that:

a. No unauthorized hardware or software is used. All software must be registered to the Department or the individual operator.

b. No free software, shareware or public domain software will be used on any department computer in order to avoid the introduction of computer virus.

c. Personal computers are located in areas secure from tampering.

d. No unauthorized upgrades, changes, additions, or repairs are made to the unit's personal computer.

4. Computer Supplies:

a. All computer supplies will be ordered from the Information Systems Division (ISD) except computer paper.

b. Computer paper can be obtained from the Police Warehouse.

B. Computer Coordinator's Duties

1. Coordinators will oversee the daily operation of a unit's personal computers and ensure that personnel using personal computers are doing so in a manner that does not damage hardware and software or corrupt data.

2. Assist Commanding Officers in matters related to personal computers and assist personnel that have not been trained.

3. Maintain a list of all personnel that are authorized to use the unit's computers or have received computer training.

4. File and update all materials, manuals, and documents related to personal computers.

5. Troubleshoot all computer related problems and work with the ATU or ISD to resolve them. Only ISD personnel are authorized to perform or order repairs on Department computers.

6. Ensure that all files are backed up.

a. Data files on hard disks must be backed up at least weekly.

b. All back-up copies of installed software and any applications programs are current, properly documented and available.

c. Assist users, as necessary, to make an up-to-date second copy of any floppy disks on which work is stored.

7. Computer Failures

    a. When a computer fails to operate properly, the computer coordinator will first contact the ATU.

    b. If it is determined that the problem is not software or user error, ATU will refer the coordinator to ISD.

C. Personnel Using Personal Computers

1. Personnel using computers will not eat, drink or smoke in the vicinity of the computers and ensure all hardware is protected from dust and liquids.

2. Maintain a current back up on a separate floppy disk or hard disk of all work.

3. Use surge protectors at all times.

D. Privately-Owned Computers

1. Employees will not be requested or required to provide a privately owned Computer the City will not repair, upgrade, or service privately owned computers.

2. Commanding Officers who permit the use of privately owned computers must:

    a. Submit a memorandum to the Commanding Officer, ISD, listing the make, model and serial number of the machine and the name and payroll number of the owner.

    b. Ensure that the software on the machine is registered to the computer's owner or the Department.

    c. Duplication of Department software on private computers is prohibited. Commanders must submit a request, in writing, through the chain of command to the Deputy Commissioner, Organizational Services, for additional serialized software.

E. Request for Hardware and Software

1. Request for hardware, software or upgrading will be submitted by memorandum through the chain of command to the Deputy Commissioner, Organizational Services.

    a. All requests must demonstrate a need for the hardware or software and include the cost and description of any peripheral equipment needed.

b. A request for software other than those taught at the ATU must include the cost of training two persons.

F. Computer Hardware Donated From Private Sources

1. Commanding Officers wishing to utilize donated equipment must submit a memorandum containing the following information:

a. Make, model and description of the equipment
b. Name of donor
c. Unit's current computer coordinator and back up
d. Required software if the request is approved

2. Commanding Officer, ISD, will review the request to determine compatibility and availability of spare parts.

3. The original memorandum and ISD's recommendation will be submitted to the Police Commissioner for their approval or disapproval.

4. Upon approval of the Police Commissioner and prior to ISD making any repairs, upgrading or software installations, the commanding officer of the unit receiving the equipment must submit a memorandum to the Police Fiscal Officer requesting a public property tag. Memorandum must include the following information:

a. Make, model and description of equipment
b. Name of donor
c. Location of equipment

---

## 3. INFORMATION SYSTEMS DIVISION (ISD)

A. In order to ensure that all personal computers, peripheral equipment, supplies and software throughout the Department are compatible and the Department's efforts are coordinated, ISD will be responsible for the acquisition, assembly and repair of all the above items regardless of their funding source.

B. User Group

1. ISD will support a mandatory user group for all computer coordinators. Coordinators will be notified by general computer message of attendance dates.

C. Custom Written Application Programs

1. ISD programmers will be responsible for the development of specialized application programs.

2. Request for Application Programs

   a. Commanding Officers requesting development of application programs must submit a memorandum to the Chief Inspector, Information Systems Bureau, outlining the reason for and goals of the program.

   b. All requests will be evaluated based on the value of the program to the entire Department.

3. ISD will maintain a library of specialized application programs available to all departmental personnel.

. Department personnel with program writing talents wishing to develop specialized application programs will:

   a. Check the ISD library to avoid duplication of effort.

   b. Provide all documentation required by ISD. (Contact ISD for specific requirements.)

5. ISD will ensure that the author's name is not removed from the documentation of the application program.

6. All programs submitted to ISD will become the property of the Philadelphia Police Department.

---

## 4. ADVANCED TRAINING UNIT

A. The Advanced Training Unit (ATU) will be responsible for training Police Department personnel in the use of personal computers, monitoring the training needs of the Department and addressing software related problems.

B. Personnel who demonstrate a working knowledge of personal computers and the Department software need only be evaluated by the ATU.

C. ATU will maintain a list of Department personnel who have been trained or evaluated.

D. Employees, who have software related problems or questions regarding software, will direct their questions to ATU.

   1. ATU will only be responsible for problems related to the following software:

a. MS-DOS
b. TEXTRA
c. DBASE III
d. LOTUS 1-2-3

---

**BY COMMAND OF THE POLICE COMMISSIONER**

---

# PHILADELPHIA POLICE DEPARTMENT DIRECTIVE 7.12

## APPENDIX "A"

| Issued Date: 03-28-12 | Effective Date: 03-28-12 | Updated Date: |
|---|---|---|

**SUBJECT: E-MAIL USAGE POLICY**

## 1. PURPOSE

A. Access to the electronic mail (e-mail) provides a means for the Philadelphia Police Department employees to communicate quickly and effectively with members of the Department and non-members about work-related City of Philadelphia business. The Department's e-mail presence affords an authorized user direct links to the public and facilitates collaborative work among City Departments/agencies.

B. Authorized Philadelphia Police Department employees are encouraged to use this technology to improve the quality and effectiveness of City services. The purpose of this policy is to ensure that the use of the City's and Philadelphia Police Department's e-mail resources is for approved City of Philadelphia business consistent with Philadelphia Police Department goals of disseminating information, encouraging collaborative projects, aiding residents and businesses, and building a broader infrastructure in support of professional, work-related activities.

## 2. GENERAL GUIDELINES

A. All City *information systems*, including *messaging systems*, are exclusively the property of the City. All *information*, including *messages*, that are created, received, transmitted, stored, deleted, and/or otherwise processed using City *messaging systems* and other City *information systems*, is considered the property of the City. All are intended to be used to conduct the official business of the City. City *information users* have no right to privacy with respect to any such *message* or other *information*, and should not expect or assume privacy or *confidentiality* with respect to any such *message* or other *information*. All such systems and *messages* are subject to access, *monitoring*, inspection, investigation, disclosure to an investigative authority, and retention by the City at any time and without advance notice to *user*, all in accordance with City *policy* and applicable federal, state and City laws and regulations.

B. All authorized users must adhere to the provisions of this E-mail Usage Policy and the city's e-mail usage policy. All users of Department e-mail must read and electronically acknowledge receipt and understanding of these Usage Policies.

C. Distributing unauthorized information regarding other users' passwords or security systems is prohibited. Unless authorized, access to e-mail accounts is restricted to the user of each account.

D. Distributing confidential and privileged criminal justice information, such as victims, witnesses and suspect identifiers is prohibited until such a time that the e-mail system is encryption enabled.

E. All authorized users must report promptly any breaches of computer security to their Commanding Officer. Upon notification, the Commanding Officer will investigate & take appropriate action (i.e. training, disciplinary action, and/or contacting the Internal Affairs Division.)

F. All authorized users of the City of Philadelphia and the Philadelphia Police Department's e-mail resources must be in compliance with all federal, state and local laws. Use of these resources must also conform to all City of Philadelphia ordinances and policies, and the Philadelphia Police Department's existing written policies. This includes, but is not limited to, the City of Philadelphia's policy and policies prohibiting discrimination/harassment which is based on race, ethnicity, color, sex, sexual orientation, gender identity, religion, national origin, ancestry, age, physical or mental disability (or a perception of such disabilities), marital status, familial status, genetic information, or domestic or sexual violence victim status or because of an association with a member of any of these protected classes.

G. City and Philadelphia Police Department e-mail resources are to be used for Philadelphia Police Department business only. This includes correspondence with professional organizations.

H. Users of City and Philadelphia Police Department e-mail resources must not download software of any kind without the prior approval of the Information Technology Director. This approval will be requested via memorandum through the chain of command and addressed to the Director, Information Technology.

I. All e-mail may be subject to Disclosure and Discovery in Litigation. Discovery production can include all e-mails and any attached data or reports in the e-mail. Labeling an e-mail as "confidential" or "privileged" will not, in and of itself, prevent the e-mail from being produced in a lawsuit.

J. In order to preserve the attorney-client privilege, messages to and from attorneys in the Law Department or otherwise acting as attorneys for the City should never be sent to distribution lists or forwarded to anyone else within or outside the City.

K. Proper business etiquette should be maintained when communicating via e-mail. When writing e-mail, Police Department Personnel (Sworn or Civilian) should be as clear and concise as possible and avoid remarks, expressions, or attempts at humor that could be misconstrued or misinterpreted. E-mail communications should resemble typical professional/respectful business communications and contain the following disclaimer:

> ***"The attached Philadelphia Police Department policies and/or information are being forwarded to you for review and are to remain confidential and privileged. The unauthorized distribution of the attached document(s) or information within is strictly prohibited."***

L. Overtime is not authorized for the handling of business e-mails while off-duty.

---

## 3. PROPER USAGE

A. Communicating with other government employees, businesses and the public in direct support of work-related functions. This includes the use of e-mail to transmit work-related documents, files and correspondences between authorized users. Police Department Personnel will not use e-mail to circumvent the chain of command. All communication via e-mail must comply with existing Department policies regarding information dissemination.

B. Informing the public about, and promoting, Philadelphia Police Department programs and services related to a user's job functions as authorized by your Commanding Officer.

---

## 4. PROHIBITED USAGE

A. Use of e-mail for illegal or unlawful purposes, including but not limited to copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal financial schemes, and computer tampering (i.e. spreading of computer viruses).

B. Concealment or misrepresentation of names or affiliations in e-mail messages.

C. Unauthorized access, alteration of source or destination addresses of e-mail, or misrepresentation of Police Department e-mail systems and the messages contained therein.

D. Initiating actions which interfere with the supervisory or accounting functions of the system, including attempts to obtain "system" privileges.

E. Causing congestion of police department e-mail systems by such things as the propagation of chain letters, broadcasting inappropriate messages (e.g., unsolicited personal views on social, political, religious, or other non-business matters) to lists or individuals, etc.

F. Use for any commercial purposes, for financial gain, or in support of "for profit" activities.

G. Promote a political party, campaign, or candidate.

H. Engaging in any activity that would discredit the Police Department or the City of Philadelphia, including seeking, transmitting, collecting, or storing defamatory, discriminatory, obscene, harassing, or intimidating messages or material.

I. Use for posting to external newsgroups, bulletin boards, or other public forums, unless it is a business-related requirement and appropriate office approvals have been obtained.

---

## 5. CONFIDENTIALITY, MONITORING, AND ENFORCEMENT

A. Inappropriate use of the City of Philadelphia or Philadelphia Police Department e-mail resources, in violation of this policy, and any unauthorized access or improper use of e-mail may subject violators to criminal, civil, and/or disciplinary action up to and including dismissal.

B. Users may not share e-mail access with anyone unless authorized to do so, and may not disclose the contents or existence of City of Philadelphia or Philadelphia Police Department computer files, e-mail, or other information to anyone other than authorized recipients.

C. Users do not have a personal privacy interest in anything created, received, or stored on City of Philadelphia or Philadelphia Police Department e-mail systems.

D. The City of Philadelphia and the Philadelphia Police Department have the right to search all e-mail use without prior notification and at any time.

1. Access or use of this e-mail system constitutes consent to the above terms.

---

**BY COMMAND OF THE POLICE COMMISSIONER**

---