


PBP FORM 290  PITTSBURGH BUREAU OF POLICE <i>"...accountability, integrity and respect."</i>		SUBJECT: "ELECTRONIC COMMUNICATIONS/COMPUTER NETWORK POLICY"		ORDER NUMBER: 68-1
		PLEAC STANDARD: NONE		PAGE 1 OF 5
RE-ISSUE DATE: 03/06/2015	EFFECTIVE DATE: 03/06/2015	ANNUAL REVIEW DATE: MARCH	RESCINDS: ALL PREVIOUS	AMENDS: N/A

1.0 POLICY OR PURPOSE

- 1.1 It is the policy of the Pittsburgh Bureau of Police to ensure that all components of the City's computer network (e-mail, Internet/Intranet access, hardware, software, etc.) are used solely for legitimate law enforcement purposes, or for endeavors that would be in compliance with the mission and vision of the Pittsburgh Bureau of Police. Members of the Bureau of Police are reminded that they have certain responsibilities that apply to the use of these components.
- 1.2 The purpose of this policy is to provide guidelines as to the proper use of all components of the City's electronic communication systems, including, but not limited to, desktop and laptop computers, tablets, mobile devices and Mobile Data Terminals.

2.0 COMPUTER SYSTEMS ACCESS AND SECURITY

- 2.1 No individual will be given access to any aspect of the PBP computer systems without the written consent of their commanding officer.
- 2.2 The commander shall designate who is authorized to use the computer systems, and designate which systems and hardware components will be available to each individual under his/her command.
- 2.3 Each authorized individual will be responsible for maintaining their own private password, and this information shall not be divulged or disclosed to any other individuals, except for legitimate law enforcement purposes.
- 2.4 When an employee is finished using a computer, the individual must log off of the computer system following the procedures set forth by the Department of Innovation and Performance (DI&P) to ensure that security breaches do not occur.

3.0 REPORTING OF STATUS CHANGES IN ACCESSING COMPUTERSYSTEMS

- 3.1 Any change in the computer access status of a member of the Bureau of Police that will necessitate a change in access rights to the City of Pittsburgh electronic computer system, such as temporary assignments, permanent transfers or promotions, must be requested in writing through the member's commanding officer.
- 3.2 This request shall be completed by the member on PBP Form #70.1 "DI&P Computer Services Request Form" and forwarded to the member's commanding officer at least one (1) week prior to the effective date of the change in status.
- 3.3 The request will then be signed by the commanding officer and forwarded to DI&P.

4.0 USE OF CITY ELECTRONIC COMMUNICATIONS SYSTEMS FOR WORK-RELATED PURPOSES ONLY

- 4.1 PBP e-mail and/or Internet/Intranet service is not to be used for personal or political purposes, and is to be used for performing lawful City business purposes only.
- 4.2 All City communications systems hardware, software, temporary/permanent files, and any related systems or devices used in the transmission, receipt or storage of e-mail/Internet/Intranet information are the property of the City of Pittsburgh.
- 4.3 Information transmitted or stored on City electronic communications systems is accessible by management with or without prior notice to employees.

4.4 All e-mail transmissions, World Wide Web browsing requests, file transfers, or other forms of electronic communications may be logged for administrative and/or security purposes. This information may be made available to individual department managers.

5.0 COMPUTER/NETWORK PHYSICAL LOCATIONS

5.1 All computers or automated equipment shall be located in an area where there is no public access. If the physical layout of the work area prohibits this, measures shall be taken to ensure that the equipment is carefully monitored in order to prevent unauthorized access or tampering.

6.0 E-MAIL-GENERAL RESPONSIBILITIES

6.1 All PBP members must read their e-mail on every working day. *(Refer to Chief's Order #98-042).*

6.2 All PBP members are responsible for the maintenance of their e-mail mailboxes. Subfolders (e.g. Inbox, Deleted Items, and Sent Items) should be routinely cleared of old e-mail to allow new messages to be sent to the Inbox. Members unsure of how to delete unwanted/unnecessary messages should contact the DI&P Help Desk at extension [REDACTED].

7.0 HARMFUL OR OFFENSIVE E-MAIL COMMUNICATIONS AND INTERNET/INTRANET TRANSMISSIONS ARE FORBIDDEN

7.1 Members of the Pittsburgh Bureau of Police will use the same professional courtesy in e-mail/Internet/Intranet communications as is used in other verbal or written communications. The tone and content of all e-mail correspondences shall remain businesslike and will not include inflammatory remarks or inappropriate language.

7.2 E-mail and/or the Internet/Intranet shall not be used in any way that may be seen as illegal, offensive, harmful, inappropriate or insulting to any person. Examples of inappropriate uses of e-mail/Internet/Intranet communications include, but are not limited to:

- Any communication that contains ethnic or racial slurs.
- Any communication that contains vulgar or profane language.
- Any communication that contains sexually explicit photography, messages or jokes/cartoons, unwelcome propositions or love letters.
- Any communication that causes congestion of the e-mail system such as chain letters, the broadcasting of inappropriate messages to global lists of recipients or other mass electronic mailings.
- Any use that does not meet the primary goals or interests of the Bureau of Police.
- Any other transmission that may be interpreted to be harassment or disparagement of others based on their race, color, religion, ancestry, age, national origin, place of birth, gender, sexual orientation, familial status, or disability status.

7.3 No member shall send or forward messages that have been altered in order to deceive the receiver as to the original content.

7.4 No member shall send or forward e-mail mass electronic messages Bureau-wide or City-wide without the approval of his/her commanding officer.

7.4.1 If a member has a legitimate need or request to deliver an electronic message Bureau-wide or City-wide, he/she shall forward the message through the chain of command to his/her commanding officer. The commander will then forward the message in mass format to all recipients if deemed appropriate.

8.0 TAMPERING WITH THE SECURITY OF COMPUTER NETWORK, EQUIPMENT, AND INFORMATION RESOURCES IS PROHIBITED

- 8.1 No member of the Pittsburgh Bureau of Police will tamper with the security of computer/network equipment, files or e-mail records of any other employee, nor will they access those files or pieces of equipment without authorization.
- 8.2 Attempts to bypass City computer/network security controls (i.e., using unauthorized passwords, etc.) are forbidden.
- 8.3 Electronic "snooping" to satisfy curiosity about other individuals is forbidden. Unauthorized software installation on any City computer/network is forbidden and the unauthorized software will be removed without notification.

9.0 COMPUTER/NETWORK EQUIPMENT HANDLING AND USE

- 9.1 Care shall be taken at all times when handling computer equipment and no time should anyone intentionally, recklessly, or maliciously attempt to cause any physical damage or remove any computer equipment without authorization.

10.0 COMPUTER/NETWORK EQUIPMENT RELOCATION

- 10.1 All computer/network equipment is the property of the City of Pittsburgh; it shall not be removed from the designated area to which it is assigned without prior authorization.

11.0 COPYRIGHT INFRINGEMENT AND PLAGIARISM ARE FORBIDDEN

- 11.1 No member of the Pittsburgh Bureau of Police will use City electronic communications systems to copy, transmit, or plagiarize information and/or software protected by copyright laws and/or licensing agreements without copyright authorization.

12.0 UNAUTHORIZED CHANGES TO COMPUTER CONFIGURATIONS AND STANDARDS

- 12.1 Installation of privately owned software onto a computer owned by the City of Pittsburgh is strictly prohibited unless authorization to do so has been granted by the Department of Innovation and Performance (DI&P).
- 12.2 Software is generally copyrighted, and the City and PBP use that software under license agreements. Misuse of software may result in violation of state or federal laws, including copyright laws and breaches of license agreements.
- 12.3 The Bureau of Police will not tolerate the use of unauthorized software copies on City-owned equipment, ~~or~~ unauthorized use of city-licensed software in any form. Computers will be periodically checked for unauthorized software, and if any such software is found it will be removed.
- 12.4 Any document, application, database or other program developed or produced on a City-owned computer becomes the property of the Pittsburgh Bureau of Police.
- 12.5 System Administrators reserve the right to delete documents, applications, databases or other programs that may be in violation of this order. If exceptions are required, the Chief of Police or his/her designee must first approve them, and DI&P must be made aware of those exceptions.

13.0 ERRONEOUS DATA ENTRY

- 13.1 Falsifying, altering, or deleting police information from any database that would cause any record or report based on such data to be false, incomplete, misleading or not of complete value is strictly prohibited.

14.0 CONFIDENTIAL INFORMATION MUST BE HANDLED APPROPRIATELY

- 14.1 Members of the Pittsburgh Bureau of Police shall avoid using electronic communications systems to send confidential, privileged, and/or sensitive information.

- 14.2 Because of the reduced effort that is required to redistribute such information, employees must exercise a much greater degree of caution in transmitting confidential information by e-mail and/or the Internet/Intranet.
- 14.3 Confidential information must never be transmitted to anyone who is not authorized to know or receive such information. To reduce the possibility that confidential information may be sent inadvertently to the wrong person(s), members should avoid the use of "multiple distribution" lists when sending information.
- 14.4 Members should insure that "current" distribution lists are used. Each name on a recipient list should be reviewed before each transmission to ensure that all recipients have a need to know and are authorized to receive the information.
- 14.5 Some examples of information which may be considered confidential include, but are not limited to:
- Personnel related matters
 - Investigations within the Bureau of Police that are of a sensitive nature
 - Confidential correspondences related to methods to be employed in dealing with crime trends or problems
 - Arbitration proceedings or contract negotiation information
 - Information relating to legal advice, questions, proceedings, or proposed legislation

15.0 MOBILE COMPUTERS

- 15.1 All current electronic communications policies/procedures will apply to the use of the laptops, tablets, and other mobile devices.
- 15.2 All current J-Net policies/procedures will apply to the use of laptops; tablets and mobile devices (*Refer to G.O. #51-1.*)
- 15.3 Except for exigent circumstances, laptops, tablets and mobile devices shall be carried in the storage case at all times.
- 15.4 Laptops, tablets and mobile devices shall not be left in the passenger compartment of the vehicles. If it becomes necessary to store in the vehicle, laptops, tablets and mobile devices shall be stored in their case in the locked trunk of the vehicle.
- 15.5 Laptops, tablets and mobile devices shall not be stored in the vehicle for long periods of time, including shift-to-shift or overnight.
- 15.6 Lost or stolen laptops, tablets and mobile devices shall be reported immediately to City Department of Innovation & Performance (DI&P).
- 15.7 Employees should not clean the screen of the laptops, tablets and mobile devices with any ammonia-based products. A damp cloth may be used to remove surface dirt.
- 15.8 Laptops, tablets and mobile devices assigned to the Investigations Branch:
- 15.8.1 The squad sergeant is responsible for maintaining a sign-out/sign-in log. Laptops, tablets and squad-maintained mobile devices shall be returned at the end of each shift.
 - 15.8.2 The squad sergeant is responsible for checking the condition of the laptops, tablets and mobile devices on a daily basis.
 - 15.8.3 Detectives shall report any damage or malfunctions to the squad sergeant who will notify DI&P.
 - 15.8.4 Lost or stolen laptops, tablets or mobile devices shall be reported immediately to the squad sergeant who must make an immediate notification to the DI&P HelpDesk.

16.0 MOBILE DATA TERMINALS (MDT)

- 16.1 All current electronic communications policies/procedures will apply to the use of the MDTs.
- 16.2 All current J-Net policies/procedures will apply to the use of the MDTs (*Refer to G.O. #51-1.*)

- 16.3 At the beginning of each shift, officers shall check the MDT to ensure that it is in proper working condition. If officers notice any damage to the hardware or software, they shall immediately report the damage to their immediate supervisor, who will promptly notify DI&P.
- 16.3.1 Once the damage has been documented, the shift supervisor shall initiate an investigation into the source of the damage to the MDT or other computer equipment. If necessary, the shift supervisor shall request that Commander in charge of the Unit coordinate a further investigation of the incident.
- 16.4 Only officers who have been certified on CLEAN/NCIC are to use the MDT.
- 16.4.1 If an employee allows either authorized or unauthorized personnel access to the system by giving their USER ID and password, this will result in removal of the employee's access to the CLEAN/NCIC system.
- 16.5 Information obtained from CLEAN/NCIC shall not be disseminated outside of the criminal justice system (*Refer to G.O. #51-1*).
- 16.5.1 Violation of the CLEAN/NCIC security can lead to the termination of the operator's access to CLEAN/NCIC privileges. An officer whose access to CLEAN/NCIC is terminated is no longer permitted to be in any area where access to information provided by CLEAN/NCIC is possible, so a violation of this section subjects that member to discipline, up to and including termination.
- 16.6 All positive indications ("hits") on persons or vehicles must be confirmed/verified through Index prior to any arrests/recoveries.
- 16.7 All information accessed, including "Logon", CLEAN/NCIC queries, and messages are logged to a database.
- 16.7.1 Reports can be produced listing all Usernames, CLEAN/NCIC queries, and messages for auditing purposes.
- 16.8 No software is to be loaded onto the MDTs without the approval of DI&P.
- 16.9 Do not modify, add, or delete any software installed on the MDT.
- 16.9.1 This includes desktop settings, applications, configurations files, icons, or any network settings.
- 16.10 All of the MDTs are locked onto the docking stations in the vehicles and cannot be removed without a key.
- 16.11 When the vehicle is in operation, the MDT should be adjusted to the low or middle telescopic position.
- 16.11.1 Due to safety concerns, the MDT should not be in the highest telescopic position unless the vehicle is parked.
- 16.12 Do not use ink pens, cuff keys, etc. to navigate the touch screen. Use only the supplied stylus, the mouse pad, or your finger.
- 16.13 When exiting the vehicle on calls, place the screen/lid in the down position. If exiting for an extended period of time, log-off.
- 16.14 At end of your tour of duty, log off all programs and shut down the laptop from the start button as you do on the station PCs. Reset the MDT to lowest position between the seats, close and latch screen/lid.

Approved By:

Cameron McLay
Chief of Police

Date: