ELIZABETH POLICE DEPARTMENT
GENERAL ORDERS

VOLUME: 5	CHAPTER: 15	# OF PAGES: 6

SUBJECT: COMPUTER, ELECTRONICS & INTERNET USAGE

EFFECTIVE DATE: **February 1, 2016**	ACCREDITATION STANDARDS: **N/A**
BY THE ORDER OF: **Chief Patrick Shannon**	
BY AUTHORITY OF: **Police Director James Cosgrove**	
SUPERSEDES ORDER #: 154	

PURPOSE The purpose of this general order is to codify this department's policy, restrictions, and procedures concerning Internet, computer, and other electronic device usage.

POLICY It is the policy of the Elizabeth Police Department that all employees abide by the guidelines set forth herein when using personal computers and the services of both internal and external data bases and information exchange networks and where applicable, voice mail, and related electronic messaging devices.

The Elizabeth Police Department may assign to its employees agency-owned computers for business purposes. This computer equipment, peripheral equipment, exchange networks, databases (internal and external) and the data stored within are and remain the property of the Elizabeth Police Department.

It is further the policy of the Elizabeth Police Department that any data stored on an agency-owned computer or electronic device is the intellectual property of the Elizabeth Police Department.

It is further the policy of this department to adhere to the tenets of the New Jersey *Attorney General's Guideline concerning Law Enforcement Computers*.

PROCEDURES

I. GENERAL PROVISIONS

A. For purposes of this general order, the terms computer, electronic device, email, and/or data or database shall refer to Elizabeth Police Department owned or leased devices, equipment or data. These devices include, but are not limited to:

1. CAD and incident records management system (including main server applications);

2. Applications and programs (e.g., Word, Excel, Access, PowerPoint, etc.);

3. Email applications:

4. Internet/Web browser applications:

5. Paging systems;

6. Electronic bulletin boards;

7. Computers;

8. Telephones;

9. Copiers;

10. Databases;

11. Exchange networks;

12. Printers;

13. Facsimile (fax);

14. External hard drives;

15. Data storage media;

16. USB Drives.

B. The availability and use of the personal computer within the work environment has provided many opportunities for enhancement of productivity and effectiveness. These technologies also entail the opportunity for rapid transfer and broad distribution of sensitive information that can also have damaging effects on this department, its members and the public if not managed properly.

C. Computers, its contents, and any electronic correspondence originating from or arriving at the computer are the property of the Elizabeth Police Department and intended for use in conducting official business with limited exceptions noted elsewhere in this general order.

D. Transmission of electronic messages and information on communications media provided for employees of this department shall be treated with the same degree of propriety, professionalism, and confidentiality as official written correspondence or public records.

1. All personnel are required to keep their email inbox current, deleting unnecessary mail.

2. All personnel are requested to notify the training division with questions concerning routine maintenance issues or routine problems.

E. Communications sent by e-mail or other electronic delivery systems may be subject to disclosure under the N.J.S.A. 47: 1A-1 et seq., or thorough standard discovery through the rules of the court. No employee shall have any expectation of privacy with regard to any information on the computer systems.

1. This department encourages authorized and trained personnel with access to information systems (IS) to utilize these devices whenever necessary. However, all these devices are the property of the City of Elizabeth and this department and use of any of these devices is a privilege that is subject to revocation.

2. Employees do not maintain any right to privacy in any department or city information system and related equipment or its contents, to include personally owned software (if approved) and email messages.

3. The department reserves the right to access any of the records within the system at any time and to retain or dispose of those records as it deems necessary and appropriate, and may require employees to provide passwords to files that have been encrypted or-password protected.

4. The department reserves the right to access, for quality control purposes and/or for violations of this general order, data, electronic and voice transmissions of employees conducting business of this department.

5. Accessing or transmitting materials (other than that required for business) that involves the use of obscene language, images, jokes, sexually explicit materials, or messages that disparage the department, any person, group, or classification of individuals is prohibited whether or not a recipient has consented to or requested such material. Exceptions:

a. Officers and detectives conducting criminal investigations that involve computer crimes can receive, copy or download sexually explicit material as long as the receipt, copy or download is a necessary component of the investigation.

b. Officers and detectives conducting homeland security investigations or intelligence gathering can receive, copy and/or download prohibited material as long as the receipt, copy or download is a necessary component of the investigation or intelligence function.

6. Confidential, proprietary, or sensitive information may be disseminated (or made available through shared directories or networked systems) only to individuals with a need and a right to know and when there is sufficient assurance that appropriate security of such information will be maintained. Such information includes but is not limited to the following:

    a. Transmittal of personnel information, such as salary, performance reviews, complaints, grievances, misconduct, disciplinary information, medical records, or related employee information.

    b. Criminal history information and confidential informant master files, identification files, or related information.

    c. Intelligence files and information containing sensitive tactical and undercover information.

F. No employee shall access or allow others to access any file or database unless that person has a need and a right to this information. Personal identification and access codes shall not be revealed to any unauthorized person or source. Visitors to this department are not permitted access to information systems or to gain Internet access through office computers except where authorized by the Chief of Police (e.g., authorized contractors, technicians, etc.).

G. Employees are prohibited from installing unauthorized software and from storing personal information in the computer system regardless of any password protection or encryption.

1. Employees shall not download or install on a department workstation or network terminal any software, or other materials from the Internet or other external sources without securing approval from the computer services unit in order to minimize infection by computer viruses, worms, or Trojan horses.

2. Material shall be downloaded to portable media (e.g., zip drive, USB drive, etc.) and scanned for viruses prior to being entered into any workstation or shared system.

3. In no case shall external materials or applications be downloaded directly to any shared (network) drive. When in doubt, employees shall consult the computer services unit for guidance.

4. Employees shall observe the copyright and licensing restrictions of all software applications and shall not copy software from internal or external sources unless legally authorized.

5. Any software for which proof of licensing cannot be provided is subject to removal by the computer services unit.

6. Any hardware enhancements or additions to agency owned equipment must be approved and authorized by the Director or the Chief of Police.: The computer services unit is responsible for determining proper installation procedures.

H. Employees shall not permit unauthorized persons to use this agency's computer system. To avoid breaches of security, employees shall log off any workstation that has access to the department computer network, electronic mail system, the Internet, or sensitive information whenever they leave their workstation.

I. Creating a web site on the Internet that has any appearance of officially representing Elizabeth or any of its departments is prohibited without the approval of the Chief of Police or his/her designee.

J. Using scanned images of any Elizabeth logo or from any of its departments on personal web sites is prohibited without the express written approval of the Chief of Police or his/her designee.

K. Employees are prohibited from uninstalling or deleting any software, programs, file folders, individual files or data of any type contained within the computer system related to official business. Uninstalling or deleting any software programs, file folders, individual files or data related to Elizabeth Police Department business must be in conformance with applicable records retention regulations and schedules promulgated by the New Jersey Division of Revenue and Enterprise Services, Bureau of Records Management (BRM) and with the permission of the computer services unit.

L. Installation of or access to software for purely entertainment purposes is prohibited.

M. Playing computer games during working hours is prohibited. Access to the Internet for entertainment purposes is prohibited. Internet access and use are restricted to official department business only. Exceptions to business use include the following:

1. Personal use may be permissible if limited in scope and frequency. The use must be in compliance with this general order and not be connected with a profit-making business enterprise or the promotion of any product, service, or cause that has not received prior approval from the Chief of Police or designee.

2. Employees may make off-duty personal use of agency computers for professional and career development purposes when in keeping with the other provisions of this general order and with the prior knowledge of their supervisor.

N. Hard drives and memory chips must be removed from computers, copiers and other electronic devices that are being disposed of prior to any auction, sale, or other disposition and in accordance with City of Elizabeth inventory policies.

II. TEXT TRANSMISSION TELEPHONES (TTY) FOR SPEECH AND HEARING IMPAIRED ARRESTEES/PRISONERS

A. TTY is a device, which allows messages to be transmitted over telephone line by typing. An acoustic model is located in the booking section. This device employs a standard telephone, requiring the handset be placed into two rubber cups of the TTY.

B. Any person in the custody of this department, who is speech or hearing impaired, will have an equal opportunity to contact the person of their choice. The booking officer shall ensure that any speech or hearing impaired arrestee/prisoner, who is not capable of using the standard telephone in booking, is made aware of the availability of the TTY.