Greer Police Department

General Order 230.2
Computer Management

This order consists of the following numbered sections:

August 29, 2023
CALEA 11.4.4; 11.4.5

I. Policy

This policy is intended to ensure that use of these computer and internet services among the Department's employees is consistent with Departmental and City policy, all applicable laws and the individual employee's job responsibilities. The provisions of this policy apply to all employees of the Greer Police Department, including full time, part time, temporary and volunteers.

These resources are provided to support an exchange of information and ideas between citizens, government agencies, community groups and Department employees; to provide research and education by providing access to unique resources; and to provide information about the activities and services of the Greer Police Department.

II. Virus Protection

A. All Department computers and data-storage devices are connected to the City's network that has anti-virus systems and a virus scan scheduled to run automatically. The anti-virus systems are updated on a regular basis with the latest virus definitions by the City's IT Department. Electronic data storage outside of the city network is maintained by the service provider (Axon) regarding data ownership, sharing, security, loss and recovery, retention and redundancy, reports, logistical requirements, and financial arrangements. The City's IT Department oversees the introduction of any computer software into a department computer.

B. Computers connected to the Greenville County E-911 system have anti-virus software installed that run and update according to the main system's schedule.

C. All software introduced from outside the Department are automatically scanned for virus by the City's network system.

D. E-mails are automatically scanned by the City's network system.

III. Pornography

The use of Departmental computers to view, record, broadcast or any other utilization of pornography is strictly prohibited. This includes the viewing of pornography photos, pornography videos and or pornography sound bites from the Internet or any other means. When pornographic sites on the Internet are part of an investigation, the employee's Supervisor must give prior approval and monitor the use of the site. If a pornographic site or email is accidentally opened, the employee must immediately notify his/her Supervisor.

IV. Email

Inappropriate email, such as jokes that promote racial, ethnic, religious or gender based slurs, or other potentially offensive material may not be distributed via the City's email system.

A. The City's email system is intended for business purposes.

Personal use must not interfere with normal business activities; must not involve solicitation; and must not be associated with any for-profit business activity.

B. Email must not be threatening, insulting, obscene, abusive or derogatory; include remarks that are threatening, defamatory toward any person, or constitute sexual or any other form of harassment; compromise the privacy and/or security of others; and/or create a hostile work environment.

C. Email must not be used to compromise the integrity of the Department and its business in any way.

D. There is no lawful expectation of privacy between email users. Confidentiality of any message should not be assumed. Even when a message or record is erased, it is still possible to retrieve and read the message or record. Therefore, email and online communications should not contain confidential information. Good judgment should be exercised in using the electronic transmission and distribution of information, especially if it may be deemed sensitive. Personnel issues are not to be discussed through email.

E. The receipt of unsolicited email of an obscene, derogatory, or offensive nature should be reported to the employee's Supervisor and steps to prevent access by such email addresses to the Department's email system initiated.

F. Email sent or received through the Department's system could be subject to public scrutiny under the Freedom of Information Act.

G. Employees who have been provided email capability have an obligation to read incoming messages in a timely manner and respond accordingly.

V. Confidentiality/Privacy

1. All computer systems, hardware, software, temporary or permanent files and any related systems or devices are the property of the Greer Police Department These include, but are not limited to, computers, network equipment, software, documents, spreadsheets, calendar entries, appointments, tasks and notes which reside in part or in whole on any Departmental electronic system or equipment files. The Greer Police Department reserves the right to access and disclose all messages and other electronic data sent over its electronic mail system or stored in its files.

2. The Greer Police Department has the authority to inspect the contents of any equipment; files, calendars or electronic mail at will and may extract information, files, documents, voice mail, etc for review. Reasons for review include, but are not limited to system, hardware or software problems, general system failure, a lawsuit against the Department, suspicion of a crime or violation of policy, or a need to perform work or provide a service when the employee is not available.

3. Use of computer systems and/or tools provided by the Greer Police Department shall not be accompanied by any expectation of privacy. Any use of the Internet connection may be monitored and/or captured in order to assess compliance with this policy. No notice to the employee that his/her activity is being monitored and/or captured will be given.

VI. Employee Responsibility

The use of the internet via the Greer Police Department's resources is a privilege, not a right. Any violation of the above conditions, policies and procedures may result in cancellation of that privilege and may be subject to disciplinary action. The employee is responsible for his/her actions while accessing the Department's computer network and the Internet.