USE OF EQUIPMENT AND COMPUTERS

Effective Date: **January 1, 2007**
Section: **503**

Computers and software furnished to Employees are intended for Township business purposes only. Employees may not use or access any Township property, passwords, files, software, or stored communications without authorization from their supervisor.

Springfield Township strives to maintain a workplace free from harassment and sensitive to the diversity of its Employees. Therefore, Springfield Township prohibits the use of phones, pagers, radios, computers, the e-mail system, and other electronic devices to be used in ways that are disruptive, offensive to others, or harmful to morale. To ensure compliance with this policy, usage may be monitored and Employees should be aware that there is no right to privacy in any communication conveyed via Township equipment.

The display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other prohibited displays or transmissions include, but are not limited to, ethnic slurs, racial comments, off color jokes, or anything that may be construed as harassment or showing disrespect for others.

E-mail may not be used to solicit others for commercial ventures, religious or political causes.

Springfield Township purchases and licenses the use of various computer software for business purposes only and does not own the copyright to this software or its related documentation. Unless authorized or licensed by the software developer, Springfield Township does not have the right to reproduce such software for use on more than one computer.

Employees may only use software on local area networks or on multiple machines according to software license agreement. Springfield Township prohibits the duplication of software and its related documentation. Employees are prohibited from loading any software, files, or other matter onto any Township computer without the prior approval of their Department Head or the Township Administrator.

Employees must notify their immediate supervisor, the Township Administrator, or any member of management upon learning of violations of this Policy. Employees who violate or who fail to report a violation of this Policy known to them will be subject to disciplinary action, up to and including termination of employment.

USE OF CELLULAR PHONES/PAGERS/ELECTRONIC DEVICES

Effective Date: May, 2005   **Revised: January, 2012**
Section: 505

Exempt employees who are issued Township cellular phones are required to carry and answer the cellular phone at all times. Exempt employees may also access email and other features of Township-issued cellular phones at any time.

Exempt employees may utilize the phones issued to them for personal calls so long as their personal phone usage is not excessive and does not cause the Township to exceed its airtime limitation.

Non-exempt employees who are issued Township cellular phones are required to carry and answer the cellular phones while on duty only. Use of email and other features of Township-issued cellular phones by non-exempt employees shall also be limited to on-duty hours. After hours or personal use of Township-issued cellular phones by non-exempt employees must be approved in advance by the appropriate supervisor, Department Head, and the Township Administrator.

Use of a Township issued cellular phone while operating a motor vehicle or piece of equipment in the performance of an emergency life safety essential function of their position or during the performance of other essential functions of the position requiring the full attention of the operator shall be prohibited. Employees should practice discretion and limit the use of a Township-issued cellular phone or communication device while operating a motor vehicle unless a hands-free method is used. Equipment to allow for hands-free use will be provided by the Township for all Township-issued cellular phones.

The use of a personal cellular phone while operating a Township-owned motor vehicle shall be prohibited unless utilized with a hands-free method. Equipment to allow for hands-free use will not be provided by the Township for personal cellular phones.

Personal cellular phones and other personal electronic devices, e.g., pagers, PDAs, etc. are exempt from Policy #801, Personal Damages. There will be no reimbursement by the Township for damage to personal electronic devices.

(Refer to department sections of the Personnel Policy Manual or specific department Standard Operating Guidelines for additional requirements or restrictions specific to particular departments.)

SERVICE DEPARTMENT ONLY

USE OF TOWNSHIP PAGERS

Township issued pagers must be carried at all times (24/7) from October 15 through April 15 with the exception of an employee who has requested and been granted off call time for a designated period.

INFORMATION TECHNOLOGY USE

Effective Date: February 14, 2017
Section: 509

The purpose of this policy is to provide guidelines for the proper use of department information technology resources, including computers, electronic devices, hardware, software and systems. Township employees shall use information technology resources, including computers, software and systems, that are issued or maintained by the Township in a professional manner and in accordance with this policy. Access to all Township information technology resources (as defined below) is for Township related activities only. The use of Township information resources for limited personal use may be authorized by the Township Administrator and Department Head pursuant to specific department policy or as a result of the unique nature of the employee's position.

DEFINITIONS

Computer system – All computers (on-site and portable), electronic devices, hardware, software, printers and resources owned, leased, rented or licensed by the Township that are provided for official use by its employees. This includes all access to, and use of, Internet Service Providers (ISP), the Springfield Township Employee Intranet, or other service providers.

Hardware – Includes, but is not limited to, computers, computer terminals, network equipment, electronic devices, telephones, including cellular and satellite, pagers, modems or any other tangible computer device generally understood to comprise hardware.

Software – Includes, but is not limited to, all computer programs, systems and applications. This does not include files created by the individual user.

Temporary file, permanent file or file – Any electronic document, information or data residing or located, in whole or in part, on the system including, but not limited to, spreadsheets, calendar entries, appointments, tasks, notes, letters, reports, messages, photographs or videos.

Township Intranet – The computer network, wired and wireless, which resides in all or most Township Offices and buildings that allows the sharing of computer resources.

PRIVACY EXPECTATIONS

Employees forfeit any expectation of privacy with regard to emails, texts or anything published, shared, transmitted or maintained through file-sharing software, the Township Intranet, or any Internet site that is accessed, transmitted, received or reviewed on any Township technology system.

The Township reserves the right to access, monitor, audit and disclose, for whatever reason, any message, including attachments, and any information accessed, transmitted, received or reviewed over any technology that is issued or maintained by the Township,

including the Township email system, Intranet, computer network or any information placed into storage on any Township system or device. This includes records of all keystrokes or web-browsing history made at any Township computer or over any Township network. The fact that access to a database, service or website requires a user name or password will not create an expectation of privacy if it is accessed through Township computers, electronic devices or networks.

RESTRICTED USE

Employees shall not access computers, devices, software or systems for which they have not received prior authorization or the required training. Employees shall immediately report unauthorized access or use of computers, devices, software or systems by another employee to their supervisor. Employees should not use another person's access passwords, logon information or other individual security data, protocols and procedures unless directed to do so by a supervisor.

SOFTWARE

Employees shall not copy or duplicate any copyrighted or licensed software except for a single copy for backup purposes, in accordance with the software company's copyright and license agreement.

To reduce the risk of a computer virus or malicious software infection, employees shall not install **any** software on any Township computer without the prior approval of their Department Head. Introduction of software shall only occur by designated and authorized employees and as part of the automated maintenance or update process of Township approved or installed programs by the original manufacturer, producer or developer of the software.

No employee shall knowingly make, acquire or use unauthorized copies of computer software that is not licensed to the Township while on Township premises, computer system or electronic device. Such unauthorized use of software exposes the Township and involved employees to severe civil and criminal penalties.

HARDWARE

Data stored on or available through Township computer systems shall only be accessed by authorized employees who are engaged in an approved Township related project or program or who otherwise have a legitimate Township related purpose to access such data. Any exceptions to this policy must be approved by a Department Head.

INTERNET/INTRANET USE

The preferred and default browser on all Township workstations is set to Google Chrome. Google Chrome must be used to browse the Internet unless a different browser is required by the web site or software vendor.

Internet sites containing information that is not appropriate or applicable to Township use and which shall not be intentionally accessed include, but are not limited to, adult forums, pornography, gambling, chat rooms, and similar or related Internet sites. Certain exceptions may be permitted with the express approval of a supervisor as a function of an employee's assignment.

OFF-DUTY USE

Unless otherwise approved in advance by their supervisor, employees shall only use technological resources related to their job while on-duty or in conjunction with specific on-call assignments. This includes email, and remote access to Township software and the Township Employee Intranet. Employees who are assigned Township-provided mobile phones are expected to carry such phones and to answer them while off-duty. Such usage is intended to be for emergency notification and call-ins only and should be a de minimus interruption to the employees' non-working hours.

PROTECTION OF SYSTEMS AND FILES

All employees have a duty to protect the computer system and related systems and devices from physical and environmental damage and are responsible for the correct use, operation, care and maintenance of the computer system.

Employees shall ensure Township computers and access terminals are not viewable by persons who are not authorized users. Computers and terminals should be secured, users logged off and shutdown overnight and on the weekend; and password protections enabled whenever the user is not present. Access passwords, logon information and other individual security data, protocols and procedures are confidential information and are not to be shared. Password length, format, structure and content shall meet the prescribed standards required by the computer system or as directed by a supervisor and shall be changed at intervals as directed by IT staff or a supervisor but at least a minimum of every three months.

It is prohibited for an employee to allow an unauthorized user to access the computer system at any time or for any reason. Employees shall promptly report any unauthorized access to the computer system or suspected intrusion from outside sources (including the Internet) to a supervisor. When a problem or alert occurs on an employee's system they must contact their supervisor immediately so the appropriate person to handle the alert is notified.

ENCRIPTION OF CONFIDENTIAL INFORMATION

The transmission of data which contains personal information about employees or Township residents that could be used for identity theft must be encrypted before it is sent out to any computer system outside the Township Intranet. This includes but is not limited to sending out email to Internet recipients, taking removable media off Township premises and uploading information to Internet web sites.

INSPECTION OR REVIEW

A supervisor or the authorized designee has the express authority to inspect or review the computer system, all temporary or permanent files, related electronic systems or devices, and any contents thereof, whether such inspection or review is in the ordinary course of his/her supervisory duties or based on cause.

Reasons for inspection or review may include, but are not limited to, computer system evaluation, efficiency review, malfunctions, problems or general computer system failure, a lawsuit against the Township involving one of its employees, an alleged or suspected violation of any department policy, request for disclosure of data, or a need to perform or provide a service.

VIRUS OR MALWARE INFECTIONS

All Township employees and staff must report to supervisors or IT personnel when they realize that their computer system has been hacked or is infected with a virus or malware. The computer should be turned off and disconnected from the Township network immediately until it can be cleaned or checked by IT personnel.

Because it is not always apparent when a computer gets infected by a virus, users should report any "unusual" or "out of the ordinary" behavior of their computer system immediately to be sure the computer system has not been compromised or infected.

EXPECTED USE OF COMPUTER RESOURCES

Township computer systems and resources are meant to be used by employees and staff of the Township to help them perform their daily work duties and fulfill their job description requirements, as defined by their supervisor.