Policy No. 7.18 **Effective Date: 12.13.2017**

Subject: **Communication Media / Use of Information Technology Resources**

Overview: The Township recognizes that computer systems, e-mail, the internet and other forms of information technology are valuable tools to make communication more effective and efficient. However unacceptable use of these tools can put the Township and others at risk. The following policy has been established for using the Township's Communication Media in an appropriate, ethical and professional manner.

Policy/Procedure:

- The availability and use of the personal computer, access to the Internet and use of e-mail within the work environment has provided many opportunities to enhance productivity and effectiveness. These new technologies also entail the opportunity for rapid transfer and broad distribution of sensitive information that can have damaging effects on the Township and employees using these electronic systems. Therefore, all Township employees must abide by this policy when using personal computers, services of external databases and information exchange networks, and voice mail, mobile digital terminals and related electronic messaging devices.

- Employees are expected to maintain the same standards of propriety, professionalism and confidentiality for electronic-based communication and records as written correspondence. This includes but is not limited to texts, blogs, instant messages, and social networking sites such as Facebook, Twitter or similar sites.

Definitions

- Communication Media: Communication Media includes all electronic media forms provided by the Township such as telephones, cellular telephones, smart phones, personal computers, electronic tablets, electronic mail systems, voice mail systems, paging systems, text messaging systems, instant messaging systems, electronic bulletin boards and Internet services, intranet, mobile digital terminals and facsimile transmissions.

- All data stored on and/or transmitted through Communication Media is the property of the Township. For purposes of this policy, data includes electronically-stored files, programs, tables, data bases, audio and video objects, spreadsheets, reports and printed or microfiche materials which serve a Township business purpose, regardless of who creates, processes or maintains the data, or whether the data is processed manually or through any of the Township's mainframe, midrange or workstations; servers, routers, gateways, bridges, hubs, switches and other hardware components of the Township's local or wide-area networks.

General Principles

1. With the exception of Township telephones and Township-issued cellular telephones, the use of any Communication Media for personal use is prohibited by the Township. For Township policies regarding the use of Township telephones and Township-issued cellular telephones see Use of Telephone, Voicemail and Cell Phones Policy.

2. All Communication Media including email, voicemail and Internet messages (including any technology-based messaging) are public records subject to possible disclosure to the public pursuant to the provisions of the Open Public Records Act. Employees should always ensure that the business information contained in Communication Media is accurate, appropriate, ethical and lawful. Employees are required to use the assigned municipal email account for all Township business and correspondence. The use of private email accounts for any Township business or during business hours is strictly prohibited.

3. All employees, who have been granted access to electronically-stored data, must use a logon ID assigned by the Township. Certain data, or applications that process data, may require additional security measures as determined by the Township. Employees must not share their passwords; and each employee is responsible for all activity that occurs in connection with their passwords.

4. Transmission of electronic messages and information on Communication Media provided to employees must be treated with the same degree of propriety and professionalism as official written correspondence. Township supplied e-mail accounts and Internet IDs must not be used for anything other than Township-sanctioned communications.

5. Correspondence via e-mail is not guaranteed to be private and is not private to the individual. If the Township determines that encryption software is appropriate, encryption software must be provided or approved by the Township Administrator. The Division Director must be given a copy of all passwords, and encryption and decryption "keys." The existence of passwords does not restrict or eliminate the Township's ability or right to access electronic communications. The Township, however, will not require an employee to provide a password to his or her personal account.

6. Use of Communication Media will be monitored for security and/or management reasons. Users are subject to limitations on their use of such resources.

7. The distribution of any information through Communication Media is subject to all policies and procedures applicable to dissemination of information by non-electronic means. The Township reserves the right to determine the suitability of this information.

8. No employee shall access any file or database unless they have a need and a right to such information. Additionally, personal identification and access codes must not be revealed to an unauthorized source.

9. To avoid any breaches of security, employees must lock any personal computer which has access to the Township's computer network, electronic mail system, the Internet or sensitive information whenever they leave their workstation.

Usage Rules

- The Township prohibits any employee, using Township Communication Media, from:

1. Viewing, downloading and/or transmitting materials (other than as required for law enforcement business) that are defamatory, obscene, or harassing or in violation of any Township rules or policy. Examples of forbidden transmissions or downloads include sexually-explicit messages;; unwelcome propositions; ethnic or racial slurs; or any other message that can be construed to be harassment or disparaging to others based on their actual or perceived age, race, religion, sex, sexual orientation, gender identity or expression, genetic information, disability, national origin, ethnicity, citizenship, marital status or any other legally recognized protected basis under federal, state or local laws, regulations or ordinances, whether or not a recipient has consented to or requested such material;

2. Violating policies prohibiting harassment, including sexual harassment and workplace violence;

3. Sending or receiving e-mails that are unrelated to Township business activities;

4. Soliciting business for personal gain or profit or gambling;

5. Soliciting for religious, political, charitable or other causes, unless the employee conducts such solicitation as part of their job responsibilities;

6. Using Communication Media for any fraudulent or illegal purpose;

7. Representing personal opinions as those of the Township;

8. Making or posting defamatory, vulgar, obscene or threatening remarks, proposals, or materials;

9. Uploading, downloading, or otherwise transmitting commercial software or any copyrighted materials belonging to parties outside of the Township, or licensed to the Township. Employees must observe the copyright and licensing restrictions of all software applications and must not copy software from internal or external sources unless legally authorized. The Township may remove any software for which proof of licensing (original disks, original manuals and/or license) cannot be provided.

10. Downloading or installing any software or electronic files (including sound and video files and files attached to e-mail messages), software or other materials from the Internet or other external sources onto any computer without the prior approval of the Division

Director. After receipt of approval from the Division Director and before being entered into any personal computer, drive and/or shared system, material installed/downloaded must be scanned for viruses with virus protection software approved by the Township. In no case shall external materials or applications be downloaded directly to any shared (network) drive without consulting the Division Director;

11. Installing or making any hardware enhancements or additions to Township owned equipment without the prior approval of the Division Director. The Division Director is responsible for determining proper installation procedures if approved;

12. Intentionally interfering with the normal operation of the Township's computers and/or network, including the propagation of computer viruses and sustained high volume network traffic which substantially hinders others in their use of the network. Employees must not disable anti-virus and other implemented security software for any reason, to minimize the risk of introducing computer viruses into the Township's computing environment.

13. Revealing or publicizing confidential Township information. Confidential, proprietary or sensitive information may be disseminated 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 transmittal of personnel information, such as social security numbers, performance reviews, complaints, grievances, disciplinary records, medical records or related information. In law enforcement operations, confidential, proprietary or sensitive information also includes criminal history information, confidential informant identification, and intelligence and tactical operations files.

14. Examining, changing or using another person's files, output, or user name without explicit authorization;

15. Sending anonymous e-mail messages;

16. Refusing to cooperate with a security investigation;

17. Attempting to break into the computer system of another organization or person;

18. Sharing or stealing passwords or permitting unauthorized persons to use the Township's electronic mail system;

19. Sending or posting messages that defame or slander other individuals;

20. Misrepresenting, obscuring, suppressing, or replacing a user's identity on any Communication Media. All users are personally accountable for messages that they originate or forward using the Township's Communication Media. "Spoofing" (constructing electronic communications so that it appears to be from someone else without a legitimate authorized purpose and authorized by the Administrator is prohibited.

21. Performing any other inappropriate uses;

22. Wasting time on non-Township business, including playing games on the internet or "surfing" the Web on Township time.

23. Using private e-mail accounts for Township business or during business hours.

No Expectation of Privacy

- Employees shall use Communication Media and on-line access for Township purposes only. The Township reserves the right to monitor, obtain, review and disclose all data such as e-mail messages, computer files, voice mail, Internet messages on Township Communication Media as deemed necessary and appropriate. Communication Media equipment, its contents and data, and all information gathered via on-line resources belong to the Township. Additionally, all data and information stored on Township computers belongs to the Township. Personal material and electronic data must not be created or stored on the Township's computers.

- The Township's computer system captures most communications using the Township's computers, even if not connected to the Township's internet service system and even if using a personal e-mail account and (2) all communications using the Township's e-mail system, even if created on a non-Township owned computer. The Township may inspect all computers and information at any time as necessary for the conduct of its business. Law enforcement Communication Media is subject to additional restrictions.

- The Township retains the right to monitor all on-line communications to ensure that employees pursue only appropriate business purposes. Monitoring may include, but is not limited to, review of data including e-mail content and attachments, e-mail addresses, tracking internet sites visited by each user, the frequency and time spent on the Internet by each user, blocking access to certain types of sites, and ensuring compliance with this Policy. Employees must have no expectation of privacy in any Communication Media equipment or its contents.

- By using Township Communication Media, each user agrees that the Township has unrestricted access and the right to audit and disclose all data and information communicated or stored on the Communication Media for any security, health, employment or other legitimate business reasons. Legitimate reasons also include systems maintenance, message routing, retrieval of business information, trouble-shooting hardware and software problems, preventing system misuse, protecting confidential proprietary information, insuring compliance with software license policies and complying with legal and regulatory requests for information. The existence of passwords does not restrict or eliminate the Township's ability or right to access electronic communications. The Township, however, will not require the employee to provide its password to his or her personal account.

Reporting Violations of Policy

- Employees learning of any misuse of the Township's Communication Media shall notify the Administrator. Use of the Internet is a privilege, not a right which may be revoked at any time for unacceptable use. Users who violate this policy may be subject to disciplinary action up to and including termination of employment. The Township also retains the right to report any illegal violations to the appropriate authorities.

- Each employee who has access to Communication Media will sign an Employee Agreement agreeing to abide by this policy.

Policy 7.20 A COMMUNICATION MEDIA AND

USE OF INFORMATION TECHNOLOGY RESOURCES

USER AGREEMENT

I have received a copy of the Township of Plainsboro's Policy on Communication Media/Use of Information Technology Resources. I recognize and understand that the Township's Communication Media and Information Technology Resources are to be used for conducting the Township's business only. I understand that use of these resources for personal purposes is strictly prohibited. I further understand that the Township may monitor my computer activity and that my visits to internet sites and e-mail messages are not private. This includes but is not limited to personal communications and communications of private, password-protected, web-based sites.

As part of the Township organization and in exchange for use of the Township's Communication Media and Information Technology Resources, I understand that this policy applies to me.

I have read the Communication Media/Use of Information Technology Resources Policy and agree to follow all policies and procedures that are set forth therein. I further agree to abide by the standards set in the document for the duration of my employment with the Township of Plainsboro.

I am aware that the violation of this policy may subject me to disciplinary action, up to and including termination of my employment. Further, I understand that this Township policy can be amended at any time without previous notice.

_____

Employee Printed Name

_____

Employee Signature

_____

Date

Policy No. 7.21 **Effective Date: 12/13/2017**

Subject: **Social Media**

Overview: Employees who use social media are required to abide by the following social media policy.

- Social Media and its uses in government and daily life are expanding each year. Information posted on a website is available to the public; therefore, employees must adhere to the following policy governing their participation in social media.

Social Media During Working Hours

- Only employees directly authorized by Administrator may engage in social media activity during work time through the use of the Township's Communication Media, as it directly relates to their work and provided it is in compliance with this policy. See Communication Media policy for definition of Communication Media.

Off-Duty Use of Social Media

- Employees may maintain personal websites including but not limited to Facebook, YouTube, Myspace, Twitter etc., or blogs on their own time, using their own facilities. In general, the Township considers social media activities to be personal endeavors, and employees may use them to express their thoughts or promote their ideas as long as they do not violate Township rules or policies.

Prohibited Material On Social Media

- Employees are accountable for their actions and statements which have an impact on others. A social media site is a public place. Even if a message is posted anonymously, it may be possible to trace it back to the sender.

- Employees must not make comments or otherwise communicate about coworkers, supervisors, members of the governing body, vendors, suppliers, residents or any other third party with whom they interact in the course of the work day in a manner that violates Township personnel policies or that is vulgar, obscene, threatening, intimidating, harassing, libelous, or discriminatory on the basis of (actual or perceived) age, race, religion, sex, sexual orientation, gender identity or expression, genetic information, disability, national origin, ethnicity, citizenship, marital status or any other legally recognized protected basis under federal, state, or local laws, regulations, or ordinances. Those communications are disrespectful and unprofessional and will not be tolerated by the Township.

- The posting of words, phrases, photographs, images or any kind of information on a personal web site may be grounds for the imposition of disciplinary action against the employee if the words, phrases, photographs, images or information adversely reflects on the employee's fitness for duty or constitutes a violation of the Township's personnel policies.

- Employees must respect the laws regarding copyrights, trademarks, rights of publicity and other third-party rights. Any use of the Township's name, logos, service marks or trademarks outside the course of the employee's employment, without the express consent of the Administrator is strictly prohibited. To minimize the risk of a copyright violation, employees should provide references to the source(s) of information used and cite copyrighted works identified in online communications.

Confidentiality

- Employees must not reveal or publicize confidential Township information, including, but is not limited to, personnel information, such as employee names and addresses, social security numbers, medical records or related information. In law enforcement operations, confidential, proprietary or sensitive information also includes criminal history information, confidential informant identification, and intelligence and tactical operations files. Employees are also prohibited from posting any internal work documents to social media sites. Prohibited social media activities include, but are not limited to, posting screenshots of computer stations, pictures of monitors and/or actual documents themselves containing confidential or internal Township information. When in doubt, ask before publishing.

Additional Restrictions

- No Township employee shall post internal working documents to social media sites. This includes, but is not limited to, screenshots of computer stations, pictures of monitors and/or actual documents themselves without the prior approval of the Administrator. Employees are prohibited from releasing or disclosing any photographs, pictures, digital images of any crime scenes, traffic crashes, arrestees, detainees, people, or job related incident or occurrence taken with the Township's Communication Media to any person, entity, business or media or Internet outlet whether on or off duty without the expressed written permission of the Administrator. Except in "emergency situations," employees are prohibited from taking digital images or photographs with media equipment not owned by the Township.

- For the purposes of this section, an "emergency situation" involves a sudden and unforeseen combination of circumstances or the resulting state that calls for immediate action, assistance or relief, and may include accidents, crimes and flight from accidents or crimes and the employee does not have access to the Township's Communication Media. If such situation occurs, employee agrees that any images belong to the Township and agrees to release the image to the Township and ensure its permanent deletion from media device upon direction from the Township.

Not Representing Township

- If an employee chooses to identify him or herself as a Township employee on their personal social media accounts and even those that do not should be aware that he or she may be viewed as acting on behalf of the Township, as such no employee shall knowingly represent themselves as a spokesperson of the Township, post any comment, text, photo, audio, video or other multimedia file that negatively reflects upon the Township, expresses views that are detrimental to the Township's mission or undermine the public trust or is insulting or offensive to other individuals or to the public in regard to religion, sex, race, national origin or any other protected status. Township employees are encouraged to exercise extreme caution posting photographs of themselves in uniform or in situations where they can be readily identified as Township employees.

Consequences of Policy Violation

- Violations of the Township's policies on the use of social media will subject the employee to discipline, up to and including immediate termination.

Please Note:

- Nothing in these policies is designed to interfere with, restrain or prevent employee communications regarding wages, hours, or other terms and conditions of employment. Township employees have the right to engage in or refrain from such activities.