City of Hampton
PERSONNEL ADMINISTRATIVE INSTRUCTION

DATE: May 30, 2018	**CHAPTER:** 10	**PAI No.** 1
REFERENCES: Section I	SUBJECT: Acceptable Technology Use	

I. Purpose:

The purpose of this procedure is to establish rules for the acceptable use of City technology equipment on the City’s computer network.

II. Coverage and Scope:

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, mobile devices, applications, storage media, network accounts electronic mail, web browsing, electronic data, social media, cloud services and file or data transfers, are the property of the City. These systems are to be used for official City business purposes in serving the interests of the City, and of our citizens in the course of normal operations.

Employees, officials, agencies, boards, committees, and contractors of the City will be referred to as “users” as applicable throughout this policy. All users must abide by this policy as well as local, state, and federal laws and regulations while using any City-issued devices or equipment or when used for official City business.

III. General Use and Ownership:

A. Users should be aware that the work they create on City systems remains the property of the City of Hampton. Users may access and use systems only to the extent proper access is granted by the City to particular systems. Users have no expectation of privacy regarding the use of the City’s technology systems.

B. Users are responsible for exercising good judgment regarding the reasonableness of system use. Users shall follow City and departmental policies on such use, and if there is any uncertainty, users should consult their director, manager, supervisor, or the IT Help desk.

C. All technology systems usage is subject to inspection to ensure compliance with City and departmental policies. Any suspected breeches of security shall be audited by the City Manager or designee at any time with or without notice. Users should report suspicious activity or suspected breeches to their director, manager, supervisor or the IT Help Desk as soon as it is known.

D. Many of the Information Systems used by the City require passwords. Users’ passwords should NEVER be shared with anyone, including members of IT staff, nor should any efforts be made to obtain the password of another user. If anyone requests your password, this activity should be reported to the department’s Director and IT Director immediately. Users must change their password at least every 90 days.

E. Anyone that connects to the City Network will be assigned a unique user name and password, and is expected to maintain their password. The sharing of user accounts to log onto systems is not permitted.

F. No attempt shall be made to obtain a level of rights on a system beyond what has been expressly granted. Examples of this include, but are not limited to, attempting to log onto a system with another user's login name, accessing an application or system through back-door access, or the use of hacking tools.

IV. City-Issued Device:

A. Users should never leave their workstation or device in an unprotected state. If a user anticipates being away from their workstation or device, they should lock it.

B. Any applications installed on a user's PC or device must be approved by IT and directly related to fulfilling their job responsibilities. New applications must work without requiring administrative rights on PCs or workstations.

C. Members of IT Technical Support and Engineering staffs maintain administrative level access to all network-connected PCs on the City network. Attempts to block or override this level of access are prohibited.

D. Any foreign media (CD-ROMs, USB flash drives, removable hard drives, etc.) will be scanned for viruses or other malicious content before files are opened or copied from them. Users can contact the IT Helpdesk (727-6421 or ithelp@hampton.gov) for assistance.

E. Anti-virus and/or Anti-malware software will be installed on every PC and/or device attached to the City network by the IT department. Users are prohibited from interfering with the operations of this software. This includes attempts to uninstall or disable the software.

F. The IT department will periodically conduct security scan on networks and PCs. IT will also automatically install security and other patches. Users will not make any attempts to disrupt or delete the scans or patches. Users can contact the IT Helpdesk with questions or assistance.

G. Each user has been allocated disk space on a network file server for storage. Users can access this storage by selecting their Z: drive in Windows Explorer. Users should save their documents to their network drive (either the Z; drive or other network drive or system designated by the department head) to ensure that they are backed up for disaster recovery purposes. Network storage space is for work related information only. Content of a personal nature should not be stored on City systems, services or equipment. Users should have no expectation of security or IT support for personal content stored on City devices. Personal content stored on City devices may be deleted at any time.

V. Local Area Network (LAN):

A. The Information Technology Department maintains a data/telecommunications network which enables users to conduct business as efficiently as possible. This network joins all City-owned PC's on a common communication platform, as well as enables Internet communication.

B. PCs and other network-based devices, such as printers, can only be attached to the network with approval from IT.

C. The connection of personal devices to the City network is prohibited unless approved by the IT department. This includes but is not limited to printers, faxes, monitors, PCs, laptops, storage devices, and network devices.

D. The IT Department is solely responsible for configuring devices to communicate on the network. Attempts to override IT configured settings are prohibited. IT may designate and approve individuals to configure devices. IT will require proper training and process compliance before the designation is approved.

E. Network expansion devices, such as wireless access points, switches, or hubs, are installed and managed exclusively by IT. These types of devices, when purchased through local retail stores, are designed for home use, and can introduce significant security vulnerabilities to the City network. Installation of these devices by anyone other than IT staff is prohibited.

F. Only select members of IT staff are allowed to actively monitor the City Network. The use of network monitoring tools by non-IT staff is prohibited.

VI. Remote Access:

IT provides a number of Remote Access and Virtual Private Network (VPN) solutions to its users. These are the only approved remote access services to connect to the City of Hampton's network. Department heads or their designee will approve all user remote access requests.

When a user requests a new Remote Access Connection, City IT will work with the user to select the best solution based on the user's needs and security requirements.

Any user who is connecting to the City network from their home PC is responsible for the security settings of that PC. This includes ensuring that Antivirus and Anti-malware software is installed and up-to-date with the latest definitions, and that Windows Updates are current. The IT Department may refuse any user the right to use their home computer for access to the city's network.

Vendors that require Remote Access will be provided with an appropriate and secure solution. Vendors will be required to complete and return a "Letter of Agreement for Remote Access to the City of Hampton Network" to the IT Department before Remote Access will be provided.

The use of 3rd party Remote Access tools (including GoToMyPC connections not coordinated through IT) to establish either an inbound or outbound connection between an external PC and a PC on the City network is prohibited unless approved by the IT Department.

VII. Internet/World Wide Web:

A. Web browsing and social networking activity should be limited to business-related sites.

B. Sites that stream video or audio are generally not permitted from the City network unless there is a business need.

C. IT can generate activity reports for any user when requested by a Department Head.

D. If IT discovers in the course of troubleshooting a network or PC related issue that a user's web activity is adversely affecting normal business operations, this will be reported to the appropriate manager/Department Head.

E. Sensitive information shall not be entered onto a 3rd party web form unless the site is secure. Users can quickly identify a secure site by locating a small lock icon on the bottom of their web browser. If there is any doubt, the user should contact the IT Helpdesk for assistance.

F. The use of online personal storage and file-sharing for City business work product is prohibited. This includes, but is not limited to, DropBox, Google Docs, and other similar programs. IT has available solutions for authorized users which allow for the sharing of documents on a secure City system with internal and external entities.

G. IT maintains a web filtering appliance that monitors web-related traffic on the network. Department heads or their designee may request access to blocked sites for employees where it is necessary for business functions. IT actively blocks the following types of contents.

1. Sites known to contain malware/spyware/adware
2. Advertisements/Pop ups
3. Pornography
4. Confirmed spam sources
5. Known hacking sites and sources
6. Key loggers and monitoring
7. Online gambling

8. Hidden files or encrypted files

9. Phishing and other known fraud sites

VIII. Electronic Mail (Email):

A. Email should be used for business use only.

B. Email is not designed for the transfer of large files. Files larger than 10 MB should not be sent using email. If a user must transfer a larger file to a user or a group of users, they should contact the IT Helpdesk for alternate methods.

C. Chain emails, spamming (unsolicited email sent from a 3rd party agent outside of the City), and bombing (flooding of users, groups, or systems with large email messages) are an abuse of the City's email system and are not permitted. This includes spreading email without good purpose to an individual, group, or system.

D. The use of the "City Employees" distribution group shall be limited as much as possible and should only be used for business reasons. Authorized users shall be approved by the City Manager or designee. The employee connection website is set up to be the primary vehicle for employee communications and notices; an employee may contact Marketing & Outreach to post notices. Please consult with your manager prior to using this group for any communication.

E. The "IT Department" distribution list should not be used to report issues. All IT-related issues shall be reported to ithelp@hampton.gov or by calling 311.

F. IT maintains a spam-filtering appliance, which attempts to filter out junk email from a users' inbox. However, since all spam filtering solutions are rules-based and reactive, no spam solution is full-proof. Therefore, if a user is repeatedly receiving unsolicited email, this email should be forwarded to helpdesk@hampton.gov and then deleted.

G. Phishing is a type of malicious email that appears to be from a legitimate source, such as a financial institution, that requests that you click on a web link and enter in sensitive personal information. Attackers then use the information provided to engage in identity theft. As with spam, IT actively filters phishing emails intended for City employees. However, if you do receive this type of email, simply delete it. Users may also opt to forward the e-mail to helpdesk@hampton.gov for further investigation and to notify other at-risk departments. You should NEVER respond to any email that is requesting any of the following items:

1. Social Security number

2. Credit Card numbers

3. Passwords

4. Bank account numbers

5. Information specific to the City's network or telephone system.

H. Spoofing is a technique used for spam and phishing, where the sender makes it appear that the email originated from a different source. The email may appear to be from you and also to you, or it may be to you but is not from the apparent sender. Attackers use these spoofed emails to get you to click on virus links, and also to obtain personal information from you. If you suspect you have been spoofed, simply delete the email.

I. Any correspondence disseminated through the City's email system is presumed to be for official City business and therefore City property. It may also be considered public information depending on its content. Therefore, all electronic messages sent from City email accounts will be uniform and consistent in the identification of the authors and/or senders. Email signature blocks will be limited to the following: employee name and credentials (if any), job title, department address, telephone and facsimile numbers, email address and have the option to use the City's logo or current branding. Any information included in the email signature block that is not specified in this instruction will be construed as the inappropriate use of City email. Quotes, pictures, symbols, philosophical statements, or slogans are inappropriate in City email signature blocks. A City department or organizations unit may request an exception to the standard email signature block. Requests for an exception must be submitted by the department head to the Director of Human Resources or designee in writing and will be reviewed and approved on a case by case basis. The ban on the use of all quotes, pictures, symbols, philosophical statements, or slogans in the City email signature block is content neutral, not limited to any particular expression, and consistent with the City's obligations under constitutional law principles. As use of the City email system is intended for official City business, the use of quotes, pictures, symbols, philosophical statements or slogans may give the incorrect, and in some instances impermissible impression the City officially endorses such quotes, pictures, symbols, philosophical statements, or slogans.

J. Users on the Microsoft365 email service have a mail storage limitation of 50GB. Email deletions should be made in accordance with the state's records retention laws. Please see the City's records Management Manual for more specific guidance on email deletions and retention methods. The Records Management Manual can be found on Employee Connection under http://www.hampton.gov/2663/Records-Management.

IX. Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including dismissal.