TOWN OF NORWOOD
PERSONNEL BOARD

#P-401 – IT RESOURCES AND USE POLICY

1. Purpose and Scope

1.1 The purpose of this document is to outline the Town's information technology resources and use policy with respect to access, maintenance, protection of Town data, work related and personal use, software, Town monitoring, e-mails, and internet to ensure that employee's utilize all Town supplied communication and technology tools and equipment in a lawful, appropriate, and professional manner.

1.2 This policy is in place to protect the employees and the Town. Inappropriate use of Information Technology Resources exposes the Town to liability and risks, including, virus attacks, compromise of network systems and services, use of unlicensed software and potential litigation.

1.3 Please see also the Town's Professional Conduct Policy, Policy Against Harassment and Workplace Violence Prevention Policy at www.norwoodma.gov, click Committee/Boards. Click Personnel Board and click Town Personnel Policies.

2. Applicability

2.1 This policy applies to all Full-time, Part-time, Contingent Workers, Intermittent/Seasonal/ Temporary Employees, Interns, Volunteers, Summer Hires, and all elected or appointed officials, contractors, consultants, vendors at the Town who are granted access to equipment, software, networks, etc. that is owned, leased and/or operated/maintained by the Town of Norwood, excluding employees of the School Department. Positions covered by Civil Service Law or a collective bargaining agreement are subject only to those portions of the policy which are not specifically regulated by Civil Service law or by a collective bargaining agreement.

2.2 To the extent permitted by law, individual employment agreements (new, updated or extensions) entered into after the effective date of this policy, with employees whose positions are subject to this policy, must follow all of the provisions of this policy.

2.3 This policy is intended to be consistent with any and all applicable laws. If any part of this policy is inconsistent with the law, that part of the policy shall be considered invalid, and the remaining provisions of this policy shall be construed so as to be consistent with the law.

3. Definitions

3.1 Please consult the Personnel Definitions Document (#D-100) regarding Appointing Authority, Regular Full Time Employee, Regular Part Time Employee, Intermittent Employee, Seasonal Employee, Intern, Volunteer, Summer Hire, Contingent Worker, Temporary Employee and any other applicable terms utilized in this document.

3.2 Authorized/Authorization – written or verbal approval/permission from a Supervisor or other management individual.

3.3 Improper/Inappropriate – not suitable for or consistent with the purposes or circumstances intended by a Supervisor or with Town policy.

3.4 Unauthorized – not justified by proper authority

3.5 E-mail - the electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical e-mail clients include Microsoft Outlook.

3.6 Chain E-mail - e-mail sent to successive people. Typically, the body of the note has directions to the reader to send out multiple copies of the note so that good luck or money will follow.

3.7 Flaming - the use of abusive, threatening, intimidating, or overly aggressive language in an Internet communication.

3.8 Information Technology Resources - Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, PDA's (Personal Data Assistant/Personal Digital Assistant), network accounts, e-mail accounts, web browsing, blogging, Web2.0, social networking, and FTP provided by the Town to authorized users to facilitate the completion of their jobs.

3.9 Internet Resources - web sites, instant messaging applications, file transfer, file sharing, and any and all other Internet applications and activities using either standard or proprietary network protocols.

3.10 IP Address - unique network address assigned to each computing device connected to a network to allow it to communicate with other devices on the network or Internet.

3.11 Properly Licensed Software – software installed by an authorized individual, as determined by the Town's IT Director, for use on the Town's computer system.

3.12 Sensitive Information - classified as Protected Health Information (PHI), Confidential Information or Internal Information such as data files, e-mails, voice messages pertaining to work or operations of a sensitive, private or confidential nature.

3.13 Spam - spam is unsolicited nuisance Internet E-mail which sometimes contains malicious attachments or links to web sites with harmful or objectionable content.

3.14 Unauthorized Disclosure - the intentional or unintentionally act of revealing restricted information to people, both inside and/or outside the Town, who do not have a need to know that information.

3.15 User(s) - individual(s) whether full or part-time, active or inactive, including interns, contractors, consultants, vendors, etc. who have been given access to and granted permission(s) to use Information Technology Resources.

3.16 Virus Warning – an e-mail containing warnings about virus or malware. The overwhelming majority of these e-mails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.

4. Eligibility

This Section intentionally left blank.

5. Policy

5.1 The Town of Norwood's (hereinafter referred as "the Town") information technology resources are vital to conducting town business. Town of Norwood employees are only permitted to use Information Technology Resources for purposes which are safe (pose no risk to employees or assets), legal, ethical, do not conflict with their duties or the mission of the Town of Norwood and are compliant with all other Town of Norwood policies. Usage that meets the aforementioned requirements is deemed "proper" and "acceptable" unless specifically excluded by this policy or other Town of Norwood policies.

5.2 Access and Uses

5.2.a Access and/or use of Information Technology Resources constitutes the user's acknowledgement and consent to this policy as well as his/her consent to the Town's recording and monitoring of his/her use (whether for personal or business purposes) of Information Technology Resources.

5.2.b Users are responsible for their own conduct and use of Information Technology Resources and are advised to exercise common sense and follow this policy in regards to what constitutes appropriate use of Information Technology Resources in the absence of specific guidance.

5.2.c The Town of Norwood realizes that the Town's Computer resources will from time to time be used for personal use. With this prior knowledge it is expected that the resources will be used in a thoughtful manner. Users are responsible for the proper and safe use of all Information Technology Resources as outlined in this policy.

5.2.d Users are expected to use good judgment and to follow the specifics as well as the spirit and intent of this policy: be safe, appropriate, careful and kind; don't try to get around technological protection measures; and use good common sense. Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline.

5.2.e User access to specific Internet resources or categories of Internet resources, deemed inappropriate or non-compliant with this policy may be blocked or restricted. A particular web site that is deemed "Acceptable" for use may still be judged a risk to the Town (e.g. it could be hosting malware), in which case it may also be subject to blocking or restriction. The Town of Norwood's anti-virus system is configured to not allow malicious and pornographic emails to reach the user.

5.2.f Protection - Employees must safeguard the confidentiality and integrity of Town systems (including password logons, password protected screensavers, access codes, log-on IDs) from improper access, alteration, destruction and disclosure. Employees will only access or use these systems when authorized.

5.2.g Accountability - Users are prohibited from anonymous usage of Information Technology Resources. In practice, this means users must sign in with their uniquely assigned Town of Norwood User ID before accessing/using Information Technology Resources. Similarly, modifying or obscuring a user's IP Address or any other user's IP Address is prohibited. You may not hide your identify by changing who you are in the system. Circumventing user authentication or security of any host, network, or account is also prohibited.

5.3 Personal Use - Information Technology Resources are provided solely for the conduct of the Town's business. However, the Town realizes and is aware of the large role technology (especially the Internet and email) plays in the daily lives of individuals. In this context, the Town acknowledges that a limited amount of personal use of Information Technology Resources is acceptable. As with other Town's resources, the personal use of the Information Technology Resources will be monitored by the employee's direct supervisor.

5.4 Unlawful, Inappropriate and Prohibited Uses

Employees must never use Town Information Technology Resources (such as the Intranet or Internet) to engage in activities that are unlawful, violate town policies or in any way:

5.4.a Result in the Town's liability, embarrassment, or loss of reputation

5.4.b Use of any computer device on the Town's network without the proper use of antivirus protection and without prior approval of the Computer Department;

5.4.c Install any software on a Town supplied device without prior approval of the Information Technology Department;

5.4.d Use Information Technology Resources for commercial gain (for example, messages that could be considered pyramid schemes or the selling of products);

5.4.e Access Information Technology Resources (including web browsing) for the purpose of gaming or engaging in any illegal activity;

5.4.f Transmit confidential information to unauthorized recipients;

5.4.g Inappropriately and unprofessionally behave online such as use of threats, intimidation or "flaming";

5.4.h Disparage through social media postings regarding the workplace and/or other employees of the Town of Norwood;

5.4.i View, download, or transmit pornographic material;

5.4.j Use Information Technology Resources for the creation or distribution of chain emails, any disruptive or offensive messages, offensive comments about race, gender, disabilities, age, sexual orientation, religious beliefs/practices, political beliefs, or material that is in violation of workplace harassment or workplace violence laws or policies;

5.4.k Significantly consume network and system resources for non-business related activities (such as video, audio or downloading large files) or excessive time spent using Information Technology Resources for non-business purposes (e.g. shopping, social networking, sports related sites, et al);

5.4.l Disable any and all antivirus software running on Information Technology Resources.

5.4.m Transmit charitable solicitations (unless prior authorization is obtained from the General Manager).

5.4.n Obtain auction-related information or materials unless sanctioned by the Town.

5.4.o Pose a risk to the Town of Norwood or are counter to its mission, such as malware repositories, sites advocating violence against civil society or against persons based on race, religion, ethnicity, sex, sexual orientation, color, creed or any other protected categories.

5.5 Protection and Integrity of Data

Employees must maintain the integrity of Town information and data stored on Town systems by:

5.4.a Only introducing accurate and truthful data into the Town's system that serves a legitimate Town purpose.

5.4.b Only acquiring, using, altering, disposing of, or destroying data or information with proper authorization.

5.4.c Protecting data and information stored on or communicated across the Town's systems and not accessing this data or information unless authorized.

5.4.d Protecting data and information communicated over internal or public networks (for example, the Internet) to avoid compromising or disclosing sensitive information or communication.

5.6 Virus Protection

Employees must check all electronic media, such as software, diskettes, CD-ROMs, and files for viruses when acquired through public networks (for example, the Internet) or from outside parties, using virus detection programs, prior to installation or use. If the employee suspects a virus, he/she will not use the applicable computer system and equipment until the virus is removed and will report the matter immediately to his/her supervisor and/or the Town's IT Director.

5.7 Department Heads are required to act consistent with this policy and ensure this policy is implemented consistently within their department.

5.8 In the event of an error or violation of this policy, either intentional or unintentional, the General Manager must be immediately informed. The General Manager will identify and make the proper correction(s). A violation of this policy, whether intentional or unintentional, will not change this policy, nor set a precedent in any future application of this policy.

6. Provisions

6.1 Town Monitoring

6.1.a All Information Technology systems may be monitored and/or accessed by the Town to ensure the integrity of the technology, protect against fraud and abuse, detect unauthorized access or use, and for other business purposes.

6.1.b No employee or public official has any expectation of privacy with respect to his/her use of Town-owned or controlled communications or computer systems.

6.1.c User activity with Information Technology Resources may be logged. Usage may be monitored or researched in the event of suspected improper Information Technology Resource usage or policy violations.

6.1.d The Town of Norwood's General Manager, or his/her designee, reserves the right to review any usage and make a case-by-case determination whether the user's duties require access to and/or use of information technology resources which may not conform to the terms of this policy.

6.1.e The Town of Norwood's General Manger, or his/her designee, has the overall responsibility to monitor compliance with this policy.

6.2 Investigations

6.2.a When the Town receives a complaint, the General Manager shall promptly investigate the allegation in a fair and expeditious manner using the assistance of other in-house resources deemed necessary. The investigations shall be conducted in such a way as to maintain confidentiality to the extent practicable under the circumstances. The Town's investigation will generally include a private interview with the person filing the complaint and with any known witnesses. The Town shall also likely interview the person alleged to have committed the alleged violation.

6.2.b If it is determined that inappropriate action or a violation occurred, the Town shall take action promptly. The action to be taken may include recommendations regarding disciplinary and/or other remedial action, up to and including termination, which shall be forwarded to the appropriate Appointing Authority.

6.2.c The concept of progressive discipline will apply, except in serious cases.

6.3 All users are advised that their use of Information Technology Resources, including Email, may result in the creation of Public Records. All incoming and outgoing emails are archived by the system for an indefinite period of time. It is the user's responsibility to properly manage and maintain their email accounts. Spam and Junk mail should be marked as "spam" and Public Records email should be organized and "filed" in your email account.

6.4 Users have no expectation of privacy regarding their use of Information Technology Resources.

6.5 Users are personally responsible for the use of their individual account and need to avoid revealing or sharing their account password(s). In the event that the user believes their password has been compromised, they should take the prudent steps to protect their account, namely changing their password(s).

7. Applicable Laws / Statutes

This section intentionally left blank.

The following document associated with and attached to this policy may change to meet the needs of the Town or new requirements of law. The HR Director may make the necessary document changes without changing the intent or content of this policy. Please consult the Human Resources Department for the most current version:

- #D-113 – Employee Acknowledgement of Receipt of Policy

PERSONNEL BOARD

For the Personnel Board: *David E. Hajjar* 12 / 10 / 2014

David E. Hajjar, chairman
Anne Haley, vice-chair
Willard Krasnow
Patterson Riley
John E. Taylor

TOWN OF NORWOOD

IT RESOURCES AND USE POLICY

QUESTIONS AND ANSWERS

Q1. I received permission from my Supervisor to use the Town's computer for personal use. May I download games to my computer?

A1. No, authorized limited personal use still requires you to comply with all Town standards regarding inappropriate use of e-mail and the internet.

Q2. A friend came to my office to visit and asked for my password so he could log in and use my computer to look up some town information. Is this ok?

A2. No, employees must safeguard the confidentiality and integrity of Town information and data stored, including password logons, from improper access.

Q3. I received data from another Town, as requested by my Supervisor, and stored the information on the Town's computer system. May I open up the file and print it out for him.

A3. No, employees will maintain the integrity of Town information and data stored on Town systems by protecting data and information stored on the Town's system and not accessing this data unless authorized.

Q4. I bought some software for my home computer and have the license. May I load it on my assigned Town computer after I have checked that there is no virus?

A4. No, an employee will only use approved and properly licensed software. While employees are to check software using virus detection programs prior to installation, only the Town's IT Director may approve the use or installation of any software on the Town's systems.

TOWN OF NORWOOD

IT RESOURCES AND USE POLICY

#D-113 – Employee Acknowledgement of Receipt of Policy

This policy, outlining the Town's information technology resources tools and equipment uses by all eligible individuals, has been written to provide information and guidance with regards to access, maintenance, protection of Town data, work related and personal use, software, Town monitoring, e-mails, and internet to ensure that all users utilize all Town supplied communication and technology tools and equipment in a lawful, appropriate, and professional manner. The Town reserves the right to change, add to or delete any part of this policy, at any time, as it deems appropriate, after an appropriate public hearing is held. The Town reserves the right to waive or vary any term of this policy, as it deems appropriate at any time in order to achieve its desired goals.

If changes are made to this policy, the Town will notify employees as soon as possible after the appropriate public hearing is held. Changes which are required by law will be effective with or without notice to employees.

This Policy does not, and may not be construed to create a contract with any employee.

With your signature below, you represent that you have read this acknowledgement, that you have received a copy of the Town's IT Resources And Use Policy, and that you have read and understand this policy.

I acknowledge that I have received and read the Town's ***IT RESOURCES AND USE POLICY***.

Please be advised that if you refuse to acknowledge receipt of this policy by signing below, your refusal will be documented and you are still obligated to follow and comply with this policy.

_____

Employee Name [please print]

_____ Date: ____/____/____

Employee Signature

☐ Employee _____ was unwilling to sign this document
[print name of employee]

_____ (HR Initials) ____/____/____.