The City of Norwalk provides users (this includes: employees, elected officials, appointees, volunteers who serve on agencies, boards, and commissions either full or part time, vendors, contractors, etc.) with access to various hardware, software and other resources in order to expand access to information available through the City’s databases and other information networks. This policy provides employees with guidelines regarding the use of the City’s information technology resources, including email, the Internet and voicemail.

This policy establishes acceptable use of the computer, electronic equipment (including, but not limited to, laptops, tablets, cell phones, fax machines, printers) and telecommunication technology systems and services of the City of Norwalk by each City officer, employee, contractor, consultant or any other person or entity authorized by the City to use these systems and services.

The City has the right to monitor, intercept, restrict, filter, and evaluate all usage of the City’s technology systems as permitted by law. The City’s Monitoring Policy/Surveillance Notice will be in accordance with all applicable federal and state laws, including the Public Act 98-142 (codified at Conn. Gen. Stat. Sec. 31-48d). No user has any right or expectation of privacy in anything that is created, sent, received or stored by computer (including email.), fax, cell phone (including text messages) or voicemail.

I. Code of Acceptable Use

Each user must comply with the guidelines set out in this policy. Users conducting business through email, the Internet or voicemail are representing the City of Norwalk. Therefore, all actions and communications should be conducted in a manner that is consistent with the behavior expected of employees of the City of Norwalk.

Users may not violate the privacy of others and must be sensitive to the fact that Internet news groups, chat rooms, certain email messages, Web sites and various other communications on the Internet are accessible to the public.

The following activities are prohibited uses of the City’s email, Internet and voicemail systems:

- Disclosing or transmitting City proprietary information, such as security specifics, software products or other public information via the Internet except when approved by authorized management
- Knowingly disabling or overloading any computer system or the network, or circumventing any system intended to protect the privacy or security of another user
- Deliberately propagating a virus or destructive program. Prohibited disruptions include but are not limited to propagation of computer worms, viruses or other debilitating programs, and using the City network to make unauthorized entry to any other machine accessible via the network or Internet
• Intentionally accessing, retrieving, storing, downloading or sending, for personal use, any sexually explicit, obscene or pornographic materials
• Operating or assisting a business for personal gain
• Communicating harassing statements or images of any kind, including disparagement of others based on race, gender, national origin, sexual orientation, age, disability, mental status, skin color, religious or political beliefs
• Distributing or printing copyrighted materials, including articles and software, in violation of copyright laws
• Soliciting, in any form, including soliciting money for religious, not-for-profit or political causes or campaigns or promoting any political candidate or cause. Limited exceptions may be made upon written pre-approval of both the Personnel Department and the Corporation Counsel.
• Sending statements or images that would constitute intimidation, harassment, threats, slander defamation, obscene or suggestive messages or offensive graphical images and commercial activities
• Participating in Chat Rooms or List Serves for personal use
• Sending electronic chain letters

It is important to remember that any employee engaging in unauthorized use of the City's email, Internet or voicemail systems, or the unauthorized tampering with or destruction of email messages kept as public records according to the Department’s or State of Connecticut Librarian Retention Policy shall be in violation of this policy. The employee shall be subject to appropriate disciplinary action, up to and including termination of employment.

II. Security

The City has installed components in this system to address the issue of security. Staff may only access the Internet and other external systems through the approved Information Technology Department approved connection.

Staff should not share with others their individual passwords or voicemail access codes. The only exception is that each user must provide the City’s Information Technology Department with his/her current passwords, to allow access to the system (if required). The City’s Information Technology Department will exercise all appropriate steps to protect confidentiality. All users must abide by the procedures and standards within the City’s Password Protection Policy.

III. General Computer Use

Workstations have been set up in a uniform manner. Changes may not be made to the internal configuration of the employee’s personal computer. However, users may appropriately customize their desktops to facilitate their work assignments.

Users may not install software in their individual computers or the network without first receiving express written authorization to do so from the Information Technology Department. Any software that is not properly licensed or is unauthorized may be deleted or removed without notice.

The City of Norwalk provides all approved software for systems. Contact the Information Technology department to request specific software.
IV. Last Logon Notice

Users should log out of their PC when they leave their desks and at the end of the work day. (Press the Flag key while also pressing the letter “L”). The Information Technology Department has provided layers of security to make it difficult for unauthorized users to gain access to the systems. Nevertheless, it may still be possible that someone can attempt to access the City network using a user’s account. Please make it a point to observe your last log in time in the dialog box that you use to sign in. The idea is that if you see a successful, or unsuccessful login for a time when you weren’t using the system, you will know that someone was trying to use your account. Please let the Information Technology Department know if this happens.

V. Data Storage and Cloud Technologies

All City data (files, records, documents, etc.) is to be stored on the City’s internal network or authorized and approved Cloud storage areas. Storing on the local drive (user desktop) is discouraged. Files or documents placed on the users’ desktop or stored on the local drive are not backed up by the Information Technology Department and are at risk of being lost. If you have lost a file and need something restored, contact the Information Technology Department via phone or help desk ticket. The Information Technology Department can assist users with storing files securely and password protecting files, if desired.

The City prohibits users from downloading and installing cloud applications or third-party apps without the explicit consent from the Information Technology Department. The use of file storage and/or file sharing applications such as Google Drive, Google Docs, OneDrive, and Dropbox must be approved by the Information Technology Department in order to ensure appropriate data privacy protocols and security measures are taken, and FOI and data retention protocols are met.

VI. Electronic Mail (Email)

A. General Guidelines

1. Incidental, de minimis personal communications via email are permitted. However, it is expected that each employee will insure that the volume and frequency of their personal communications do not interfere with their work assignments or the operation of the City’s mail server.

2. Users shall not use their Norwalk email account to subscribe to non-work related mailing lists, non-work related online retail sites, non-work related-newsletters, etc.

3. Employees should be aware that when sending messages from their desktop, every message is identified with their name and identifies them as an employee of the City of Norwalk.

4. Email messages are not considered confidential. All email messages that are sent or received in the conduct of public business are considered a public record and are subject to disclosure under the Freedom of Information Act.

5. Because of their public nature, all email messages and attached documents sent to or received by an employee are considered property of the City. The City reserves the right to access and to monitor all messages sent and received over email systems without notice. Email should be treated as any other shared filing system.

6. Email messages dealing with legal issues sent to or by any employee in the Office of Corporation Counsel must include a footer on each page containing material which should
remain confidential that reads as follows: “Privileged attorney-client communication. Do not forward unless authorized.” Said emails may be forwarded to other employees who are on a “need to know” bases without prior authorization.

7. No email message, written document or other communication originating from or addressed to the Corporation Counsel to any employee or officer of the City may be disclosed, disseminated, or distributed to any person or persons without the express written authorization of the Corporation Counsel.

8. To avoid disabling the City’s network, users should not send messages containing large inserted documents, clipart and photos to a large number (15+) of internal recipients. A better way to distribute information with large attachments to many recipients is to copy the file to the H: drive or other common access area and email the file location to the group, for example: H:MyLargeFiles/2018/largefile.xls. This prohibition does not apply to recipients that are not part of the City’s network, however, keep in mind that many recipient email servers will not accept files larger than 5 megabytes.

9. Incorrectly addressed email shall be sent back to the original sender with a message that the message had been incorrectly addressed. If the incorrectly addressed email is confidential, it shall not be forwarded or returned by email, but the recipient shall otherwise notify his/her department head of its receipt. The original of any misdirected email shall be deleted.

10. The email system is not intended to transmit confidential or sensitive materials, which are more appropriately communicated in written form or by personal conversation. No confidential messages or sensitive information (i.e. health information, personally identifiable information, passwords, payment information) should be sent by email. The Information Technology Department can assist users with sending encrypted, secure emails and attachments.

11. Users should not forward messages to other parties unless the content of the message warrants it (e.g. it would be more appropriate for another department to respond to the message, or another department needs to be made aware of an issue).

B. Standard Operating Procedures for Email
To ensure the reliability and integrity of our email communication system, the following guidelines and procedures should be utilized:

1. Regularly attend to your incoming mail. Check your mail on a daily basis.

2. On a regular basis, clean up the in and out boxes. Users who are uncertain whether a specific email message must be retained should Contact their department head regarding the department’s retention requirements based on the content and nature of the email. Users should be aware, however, that when they have deleted a message from their mailbox, it may not have been deleted from the email system’s back-up function.

3. When out of the office for an extended period (over 1 business day), a standard out-of-the-office email message should be configured. The Information Technology Department can assist users in setting this up.
4. Broadcast email messages must be pre-approved by a Department Head for mass distribution.

5. Use the same rules of etiquette as you would in sending a letter or memo to someone.

6. If unsolicited mail with attachments from an unknown sender is received via the Internet, proceed carefully as viruses are easily transmitted this way. Call the City's Information Technology department if you have any questions and do not open the attachment.

7. Notify the Information Technology Department if you are receiving junk, suspicious, or inappropriate mail.

C. Retention Guidelines
Retention requirements are determined by the State of Connecticut for email and City documents. Contact your Department Head for the retention requirements for your unique Department. It is the responsibility of each City Department Head to determine his/her Department's appropriate retention requirements.

VII. Internet
A. General Guidelines
1. Limited, de minimis, incidental personal use of the Internet is permitted within reason. Any such personal use must be occasional, during breaks or non-work time, shall not interfere with the user's performance or his or her job duties or City operations, or consume significant technology/system resources.

2. Access to and use of the Internet is restricted to business use of the City, by authorized users except as otherwise permitted herein. A user's Internet activities may be logged by a surveillance system and reviewed by authorized City personnel. Users who use the Internet for indecent, vulgar, harassing, fraudulent, intimidating or other unlawful purposes, or who visit web sites that contain such material, are subject to discipline, up to and including termination and for non-employee users revocation of their access and/or use of the systems.

3. Each user of a City-provided Internet account is responsible and accountable at all times for the proper use of that account. All Internet users are expected to know the tools, rules and etiquette of the Internet and to adhere to these guidelines accordingly. Users should be aware that both the technology infrastructure and their own computer track and record sites visited on the Internet and that this record is subject to review at any time.

B. Standard Operating Procedures for Internet Use
Internet access can escalate the threat of computer viruses to the integrity of the City of Norwalk's internal networks. The ultimate responsibility to prevent computer viruses rests with the end user. To ensure the reliability and integrity of our Computer/Communications Systems, the following guidelines and procedures should be utilized. (Some departments may have a different procedure that has been approved by the department head.)
1. If a virus is detected and reported, immediately contact the Information Technology Department.

2. Uploading of files to the Internet is only permitted with authorization of the Department Head or City Management. The request to upload information must contain a description of the data as well as the reasons it is being uploaded.

VIII. Voicemail

A. General Guidelines
   1. Personal communications via voicemail are permitted. However, it is expected that each employee will ensure that the volume and frequency of their personal communications do not interfere with their work assignments. As in the case of email, voicemail should not be considered confidential and may be monitored.

   2. Voicemail can be considered a type of electronic mail communication, in that the message is recorded in an audible rather than a visible format.

   3. Voicemail is transitory in nature and may generally be deleted at will. There are times, however, where voicemail or answering machine messages may require a longer retention period. This would be in the case where the message may be potentially used as evidence in a trial. Voicemail may also be subject to the discovery process in litigation.

   4. Incorrectly addressed voicemail shall be sent back to the original sender with a message that the message has been incorrectly addressed. If the incorrectly addressed voicemail is confidential, it shall not be forwarded or returned by voicemail, but the recipient shall otherwise notify his/her department head of its receipt. The original of any misdirected voicemail shall be deleted.

   5. The voicemail system is not intended to transmit confidential or sensitive materials, which are more appropriately communicated in written form or by personal conversation. No confidential messages should be sent by voicemail.

      Users should not forward messages to other parties unless the content of the call warrants it (e.g. it would be more appropriate for another department to respond to the message, or another department needs to be aware of an issue).

B. Standard Operating Procedures for Voicemail
   1. Check your messages on a regular basis.

   2. Include on your voicemail message a way for the person calling you to speak with someone directly.

   3. Update your voicemail message when you will be away from the office or unavailable for an extended period. The Information Technology Department can assist users in setting this up.
3. Update your voicemail message when you return.

4. Delete messages on a frequent basis unless otherwise indicated. This will avoid the problem of "Mailbox full" for incoming callers.

5. Answer your phone if you are in the office. Voicemail should not be used as a way to avoid taking phone calls.

IX. Enforcement

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

Non-employee users who violate this policy may have their right to access or use of the City’s technology systems revoked.

X. Document Distribution & History

This document is the property of the City of Norwalk and is distributed to all users with network access privileges for reference. Questions regarding this Acceptable Use document can be directed to the Norwalk Information Technology Department at (203) 854-7714.

Approvals:

ITT Committee: June 6, 2018

Director, Information Technology

Director, Personnel and Labor Relations

Corporation Counsel

Mayor Harry W. Rilling
XI. City of Norwalk Technology Acceptable Use Policy – Employee Receipt

Please review the above Technology Acceptable Use Policy and return this form to the Personnel Department.

I have received, read, and agree to the Technology Acceptable Use Policy of the City of Norwalk.

__________________________  __________________
Employee Signature            Date