City of Worcester
Computer Access and Usage
Policies and Procedures

All computer systems with direct access to the City of Worcester network are subject to the policies and procedures published by the Technical Services Department for, and on behalf of, the City of Worcester. The Technical Services Department has been designated as the agency of the City authorized to implement, enforce, and investigate violations of the City of Worcester Computer Access and Usage Policies and Procedures.

In order to maintain a secure computing environment in the City, the following policies and procedures relating to general computer access and usage, electronic mail, the Internet and Social Media apply to all employees and will be strictly enforced. This policy will be updated as necessary.

I. COMPUTER USAGE POLICIES and PROCEDURES

A. GENERAL

1. All City computers are the sole property of the City of Worcester. All hardware, software, files and documents contained therein are considered to be exclusively the property of the City of Worcester.

2. Laptop, tablet, iPad, smart phone, etc., users must follow all the same guidelines and policies contained within this document. Any use of and activity performed on City-owned equipment will apply to these policies.

3. All documents, emails, etc., created on a City of Worcester computer are considered public record.

4. Any unauthorized non-City use of these resources for personal or business purposes may be cited as a violation of City policy and result in possible loss of City computer access privileges and/or disciplinary action to the persons or departments found in violation.

5. No software, hardware, wiring or equipment of any kind, is to be installed, added to, or removed from City computer systems or the network without proper authorization and assistance from the Technical Services Department through a request to the Help Desk.

6. No computer equipment including, but not limited to, PC's, printers, servers, or any network components is to be disconnected or moved without authorization and assistance from Technical Services through a request to the Help Desk.

7. Technical Services must be notified in advance of any department or office relocation or renovation that will involve disconnecting computer equipment.

8. Any action by an employee to knowingly misuse the system, or intentionally compromise or corrupt the system in any way, including but not limited to loading unapproved software, is a violation of this policy and may subject the employee to disciplinary action by the City.

9. The Technical Services Department reserves the right to remove from the network at any

time, any computer system, hardware, software or user account which is deemed to be a security risk, is the source of any intrusion, or contains a virus.

10. All City departments having access to the network will be subject to periodic and unannounced computer system inspections by Technical Services in order to ensure compliance with the policies and procedures described herein.

11. All technology-related purchases must be approved by Technical Services.

12. User accounts and e-mail messages may be monitored or accessed at any time to verify that employees are utilizing their computer privileges for City business only.

13. It is the responsibility of each user to take proper measures to ensure that a virus-free, secure and uncompromised computer environment is maintained.

B. HARDWARE

1. Departments are responsible for the security of system equipment, including, but not limited to: computers, printers, laptops, mobile devices, scanners, plotters, etc.

2. City departments are responsible for the costs to purchase, maintain and upgrade custom applications and individual equipment including, but not limited to items such as PC's, laptops and the associated software.

C. SOFTWARE

1. All software must be approved and installed by the Technical Services Department.

2. Users must initiate a Help Desk request for the installation of approved software.

3. All software license agreements and copyright laws will be strictly enforced by the Technical Services Department. Software will not be installed without the associated license documentation.

4. Users are responsible for the safekeeping of licenses and documentation for all installed software. Licenses and documentation must be readily available for inspection.

5. The security of all data and programs is the responsibility of the user to whom the computer has been assigned.

6. Users are responsible for making back-up copies of important data files by copying files to: a local tape back-up unit, media, or the network server to be subsequently saved by Technical Services during normally scheduled system saves.

D. USER ACCOUNTS

1. A user account gives a person access to system and network resources.

2. The user account serves as an identification badge to access City systems. All activities in the user's account are maintained in a system log file.

3. Each user account is to be used only by the individual to whom the account has been authorized.

4. Each user is responsible for all his/her accounts and any manner in which they are used.

5. Each user account is protected by a password. Like an office key, signature stamp, or safe combination, the user password should be kept secure at all times and should not be shared with any other users.

6. Each system user will be responsible for ensuring that his/her account password is not available to any other user.

7. Users should never send passwords through electronic mail.

8. Users will be required to periodically change their passwords for security reasons. The frequency of changing passwords will depend on system, application, and/or department requirements.

9. The Windows user password must be changed every 90 days using the following password guidelines:

   Passwords must contain characters from three of the following four categories:

   English uppercase characters (A through Z).
   English lowercase characters (a through z).
   Base 10 digits (0 through 9).
   Non-alphabetic characters (for example, !, $, #, %).

   Passwords can't contain your username or display name

   Your new password needs to be a minimum of 8 characters and will continue to expire every 90 days.

10. After logging into the system, users should never leave their computer unattended, even for short periods of time.

11. Users should logout or exit from all sessions when they leave their computer.

12. Users should logout or exit from all sessions at the end of each day.

13. Department heads or their designees should contact the Help Desk when an employee is terminated so that Technical Services can deactivate all accounts of the terminated employee. If access to a terminated employee's account is required, department heads should contact the Help Desk via e-mail to request the temporary activation of the account. This will enable authorized persons to retrieve any necessary files. Requests to access a terminated employee's account should be made within 30 days of termination. All accounts of terminated employees will be deleted 30 days after the termination date and the files and data contained within these accounts will no longer be accessible.

E. HELP DESK

1. Users should notify the Help Desk regarding hardware malfunctions or other system and network problems. A Help Desk representative will work with the user to resolve the problem or forward the information to the appropriate party for resolution.
2. Users are requested to use the Online Help Desk to log a request for assistance. The Online Help Desk can be accessed via the City's Intranet. The Help Desk may also be reached by calling 799-1280, Monday through Friday, 6:30 A.M. to 5:30 P.M. The Help Desk is not operational nights, weekends or holidays. A voice mailbox has been established so that users can leave messages for the Help Desk after hours or if all phone lines are being utilized. A Help Desk e-mail account has also been created. Users can send e-mail messages to the username: "helpdesk" and a call will be logged via the online Help Desk where applicable.

3. Users should not directly contact hardware or software companies for any networked system software or equipment problems. All hardware service calls must be initiated by a Help Desk representative.

F. HARDWARE/SOFTWARE PURCHASES

1. Purchases of any hardware and/or software items must be pre-approved by Technical Services. In order to expedite this process, users should adhere to the following guidelines:

    a. Please contact Technical Services via the Online Help Desk to seek assistance with a technology-related purchase.

    b. All technology quotes for city equipment must be initiated and provided by Technical Services.

    c. Departments are responsible for the cost of annual maintenance of any new hardware or software products.

    d. All purchase orders for technology must be sent to Technical Services who would order and receive the items. Unless otherwise noted, all purchase orders for technology-related purchases must include a ship code of "680" to ensure that all equipment is shipped to Technical Services for proper inventory and installation. Once the equipment is received, a representative will contact the requestor to schedule installation.

G. SUPPLIES

1. User departments are responsible for the purchase of system supplies, such as printer cartridges and toner, paper, etc.

II. ELECTRONIC MAIL POLICY

The purpose of this policy is to offer guidance to City employees on the proper use of the City's electronic mail (e-mail) systems, as well as the management and retention of documents that are created or transmitted on the City's e-mail systems.

A. ELECTRONIC MAIL SYSTEM

1. For the purpose of this policy, the e-mail system applies to all of the City's electronic mail systems that are managed by the Technical Services Department and the Internet mail system.

B DEFINITION OF AN ELECTRONIC MAIL MESSAGE

1. An electronic mail message may be defined as a document created or received on an electronic mail system including, not only the message, but also notes, memos, files, and any other attachments that may be transmitted with the message.

C. EMPLOYEE USE OF E-MAIL

1. The City's e-mail system is to be used for official City business only. Any misuse of the e-mail system by an employee may result in disciplinary action, up to and including termination.

2. The e-mail system, inclusive of mail messages, is the property of the City of Worcester.

3. Since most e-mail messages are drafted in private, many users often think that what they are writing is private. This can be a costly and embarrassing mistake. The content of an electronic mail message is considered the same as any other written document or statement you might make**. It is subject to disclosure under the Public Records Law and in any court proceeding involving you or the City.**

4. Any statements via e-mail may subject you and the City to the same liabilities as a written statement. A good rule of thumb to keep in mind before you send any e-mail message is to ask yourself whether you would be comfortable if the public was able to read your message in tomorrow's newspaper.

5. Remember that any e-mail message you send can be forwarded to another user without your knowledge or consent.

D. E-MAIL MESSAGE RETENTION

The following retention policy applies to all e-mail user accounts within the City, without exception.

1. The Microsoft Outlook interface for the e-mail system, including the inbox, outbox, folders, and deleted items, is a temporary storage area for messages. Email messages will be saved in your email account for a period of 60 days. After 60 days, they will be deleted from the Outlook mailbox. However, as part of the City's e-mail archive system, all messages, sent and received using the city's email system, are automatically saved and retained for a period of seven (7) years on a separate email retention platform. After seven years, the e-mail message will be automatically purged from the archive system. **Please note that all incoming and outgoing email messages will be automatically saved to the archive system and can be disclosed under the Public Records Law.**

2. Saving or printing e-mail messages for retention must be performed before the purge process takes place.

3. Any user that utilizes e-mail as a vehicle for communicating with the public, or as a means of conducting municipal business, should follow the guidelines set forth by the State's Department of Public Records. Since the City's e-mail retention policy applies to all e-mail regardless of its purpose, **departments who must retain messages for the public and are unclear about the retention period for documents within their department should contact the City's Law Department for assistance.**

III. INTERNET POLICY

Employees may be provided with access to the Internet when there is a business need to do so. The following outlines the City of Worcester's procedures for establishing Internet accounts and the policies relating to appropriate use of the Internet by City employees.

A. INTERNET ACCESS DEFINITION

1. Internet access includes viewing Web sites, sending and receiving electronic mail, transmitting or receiving files, and running Internet applications.

B. ACCOUNT REQUEST PROCESS

1. Internet accounts will be issued after the following criteria have been met:

   a) An Internet User Account Request Form (available from the Technical Services Help Desk) must be completed and signed by the employee with written department head approval. The Justification for Employee Use section must be filled in by the department head.

   b) The completed Request Form should be sent to the Technical Services Department. Once the request has been approved and the Internet account established, the Help Desk will contact the employee to verify the account.

C. OWNERSHIP

1. Like the City's computers and e-mail messages, Internet accounts and associated files are also considered property of the City of Worcester.

2. The contents of a mail message sent via the Internet should be considered the same as any other written public document. Any statement via e-mail may subject the City and the author to the same liabilities as a written public statement.

3. The Technical Services Department has the authority to monitor employee activity on the Internet to ensure proper use and is responsible for reporting any misuse to the responsible department head and the City administration.

D. ACCEPTABLE USE OF THE INTERNET

1. Use of the Internet by City employees must be for City business purposes only. Employees may use the Internet for research and analysis specific to their work-related duties.

2. The Help Desk should be contacted for assistance before any employee downloads business-related files from the Internet. Technical Services reserves the right to remove any files downloaded from the Internet that are not business-related.

3. The City has the right to notify the appropriate authorities if it discovers evidence of any possible illegal activities.

4. The City's web content filter blocks websites that are categorized as inappropriate, non-business related, security risks, etc. If a work-related site you are trying to access is blocked by the web filter, you will have the option to request approval from your department head to access the site. If approval is granted, a Help Desk request will be logged to provide access to the site. Technical Services reserves the right to deny access to any site that may pose a security risk.

E. UNACCEPTABLE USE OF THE INTERNET

1. Use of the Internet for any purpose that violates federal, state, or local laws is prohibited. This includes misuse of copyrighted material (text, picture, or sound) which may be available on the Internet.

2. Use of the Internet for purposes not directly related to official work tasks is prohibited.

3. Use of the Internet for private or personal business of any kind is prohibited.

4. Downloading files, including screensavers, from the Internet is prohibited, unless work-related and approved by Technical Services.

5. Solicitation of non-City business or use of the Internet for personal gain is prohibited.

6. Use of the Internet for access to, or distribution of, pornographic and/or sexually explicit material is prohibited.

7. Use of the Internet in a sexually harassing manner is prohibited

8. Establishing links to the City's web site from an employee's personal web site is prohibited.

9. Misuse of the Internet by a City employee is cause for disciplinary action, up to and including termination of employment.

F. ACCOUNT SECURITY

1. It is the user's responsibility to ensure security of his/her Internet account.

2. User accounts may be terminated at the discretion of Technical Services if a violation of system or network security occurs.

3. Technical Services may monitor employee account activity on the Internet at any time.

4. Users should report to the Help Desk if they receive any communications, via the City's e-mail system or the Internet, that violates these rules.

IV. SOCIAL MEDIA USAGE POLICY

This policy establishes guidelines for the use of social media sites (including but not limited to Facebook and Twitter) as a means of conveying City of Worcester information to its citizens. The intended purpose of establishing a social media presence is to disseminate City information deemed useful to its citizens.

A. General Policy

1. The establishment and use of social media sites are subject to the approval of the City Manager or his designees. All City of Worcester social medial sites shall be administered by the City's Technical Services Department.

2. Access to social media sites is restricted to City employees performing official City business.

3. Department heads are responsible for determining who is authorized to use social media on behalf of the department.

4. The establishment of social media sites is limited to only those departments who have information deemed necessary to disseminate to the public.

5. City social media sites should make clear that they are maintained by the City of Worcester and that they follow the City's Social Media Policy.

6. All City of Worcester social media sites should link back to the official City of Worcester website

7. The City's Technical Services Department will monitor content on City social media sites to ensure adherence to both the City's Social Media Policy and the goals of the City.

8. The City reserves the right to restrict or remove any content that is deemed in violation of this Social Media Policy.

9. All City social media sites shall adhere to applicable federal, state and local laws, regulations and policies.

10. City of Worcester social media sites are subject to the Massachusetts Public Records Law. Any content maintained in a social media format that is relative to City business, including a list of subscribers, posted communications, and communications submitted for posting, may be a public record subject to public disclosure.

11. Comments and postings not relative to official City business may be removed at the discretion of the City of Worcester.

12. Employees representing the City of Worcester, via the City's social media sites, must conduct themselves at all times as a representative of the City and in accordance with all City policies.

13. Access to any personal social media sites using City computers is strictly prohibited.

B. Comments and Postings Policy

1. Comments containing, but not limited to, any of the following inappropriate forms of content shall not be permitted on the City of Worcester social media sites and are subject to removal.
    a. Comments not related to the original topic
    b. Profane, obscene, violent or pornographic content and/or language
    c. Content that promotes discrimination on the basis of race, creed, color, religion, age, gender or national origin
    d. Defamatory or personal attacks
    e. Threats
    f. Comments relative to political campaigns
    g. Solicitation
    h. Violations of any federal, state or local law
    i. Illegal activity

2. The City of Worcester reserves the right to deny access to the City of Worcester social media sites for any individual who violates the City's Social Media Policy.

3. Departments shall monitor their social media sites for comments requesting responses from the City and for comments in violation of this policy.

V. DATA SECURITY

1. City data should be safeguarded at all times and accessed only through the City's secure networks.

2. City data should not be copied onto a laptop or external device.

VI. SYSTEM MONITORING

1. Computer usage will be monitored for compliance of these policies.

2. Messages that contain inappropriate content are flagged by the system and automatically forwarded to the appropriate authorities.

VII. Non-City Employees

Users who are not employees of the city of Worcester, but require use of the city systems, are subject to the provisions of this Computer Access and Usage policy; however, violation of any provision of this policy may result in the termination of such user's system privileges, and further, such violation may be reported to user's employer for further action.