CITY OF MERIDEN

POLICIES

CI1Y OF MERIDEN
ACKNOWLEDGEMENT OF POLICIES

I hereby acknowledge that I have received the following City of Meriden Policies and Code of Ethics:

- Acceptable Use Policy for Information Technology
- Drug Free Workplace Policy
- Nepotism Policy
- Sexual Harassment Policy
- Tobacco Use Policy
- Workplace Violence Policy Statement

Employee/Intern Print:_____

Employee/Intern Signature: _____

Date: _____

THE CITY OF MERIDEN
ACCEPTABLE USE POLICY FOR INFORMATION TECHNOLOGY

This *Acceptable Use Policy For Information Technology* applies to all City of Meriden employees and governs access to and appropriate use of information technology and equipment during and after work hours. The City of Meriden provides an information system, information technology, and a variety of technological tools such as computers, electronic-mail ("email"), internet access, web browsers, and mobile devices to employees to enhance job performance. The *Policy* consists of the following sections:

A. Definitions
B. Computer Use Policy
C. Electronic Communications Policy
D. Mobile Devices
E. Social Media Policy
F. Additional Guidelines
G. Conclusion

A. DEFINITIONS

Access – The ability to read, change, or enter data using a computer information system.
Article – An original posting of content to a City of Meriden social media site by a City of Meriden author.
Blog/Weblog – A City of Meriden website with regular posts displaying commentary, descriptions of events, and/or other material such as graphics or videos.
City – City of Meriden.
City Business – The use of City equipment, email addresses, and communications, including commentary, in an official capacity shall constitute conducting City business.
City Author – An authorized City official or authorized employee who creates and/or is responsible for authorized posted articles and information on a social media site (see "*Article*" above).
Commentary – A response to a City article or social media content submitted by a commenter.
Employee – Any employee of the City or any other person hired or appointed by or volunteering for the City who utilizes City information systems and information technology and equipment as part of a job or task assigned.
Equipment – Cellular phones, computers, hubs, keyboards, mice, monitors, routers, software, switches, tablets, telephones, and any other information technology resource.
Information System/Information Technology ("IT") – Computer: equipment, hardware, network, software, databases; email, electronic message systems, internet access, personal

digital assistants, web browsers, and any and all information used by the City to support its operation that is generated by, transmitted within, or stored on any electronic media.
Network – Any system that transmits data with a connection to a router, server, and/or switch.
Social Media – Content created by an individual using accessible technologies through the internet. Examples of social media include, but are not limited to: Facebook, FourSquare, Google, Instagram, LinkedIn, Snapchat, Twitter, and YouTube.
Social Media Administrator – The individual responsible for the content management and maintenance of a social media page.

B. COMPUTER USE POLICY

The following is the policy adopted by the City of Meriden concerning the proper use of the City's computer systems. The goal of this policy is to be consistent with other City policies regarding the protection of City assets and to promote proper use. This statement is based on good business practice and serves as instructions for all City employees to follow when using City-owned computer resources.

Misuse of computer resources may result in the removal or restriction of computer privileges, disciplinary action through and including discharge, or both. The Department Head is responsible for overseeing employees and is responsible for disciplinary action if necessary. The IT Department acts in an oversight capacity to ensure system procedures are enforced and adhered to.

TERMS AND CONDITIONS

Internet access is available to select employees who have a demonstrated need to utilize internet resources. Your Supervisor must have given you explicit permission for access.

RESPONSIBILITIES

1. Employee internet users are expected to act responsibly in all communications, research, and retrieval functions.
2. Not all information on the internet is free. When you are asked to register at a site, make certain that you will not be charged a subscription fee. The City is not responsible for fees incurred for on-line subscriptions unless prior authorization is obtained from the Department Head.
3. You should exercise common sense when using the internet. Whenever possible, information obtained from an internet site should be verified for accuracy and timeliness.
4. The internet is a constantly changing environment. Sites become outdated, and new services appear all the time. Make every effort to ensure that you are obtaining accurate information for your Department or Division.
5. Any internet problem or security breach is to be reported immediately to the IT Department.
6. Always represent yourself as you on the internet, never anyone else.
7. Never attempt to access services or sites for which you are not authorized.
8. Inappropriate materials or materials that are not related to the work environment are not to be accessed, downloaded, or stored. The City's sexual harassment policy applies to your conduct on the intranet and internet. The use, viewing, communication, and/or

downloading of sexually explicit materials is absolutely prohibited. Behavior that is prohibited in the workplace is prohibited in cyberspace.

COMMUNICATIONS AND ETIQUETTE

All electronic communications are expected to abide by customary standards of courtesy and generally accepted principles of computing and network etiquette as well as the City's Code of Ethics.

1. Be polite, and consider the tone of your communications.
2. Be aware that the internet is an unsecure environment. Never discuss the City's business in any manner that might reveal confidential information. Never send proprietary or confidential files over the internet.
3. Do not access external computers in such a way that could be disruptive to others.
4. Assume that information at non-governmental sites is private property. While information may be free for use on-line, downloading and printing may be covered by intellectual property laws. Respect and adhere to copyright laws and fair use guidelines.

APPROPRIATE USE

IT and equipment is to be used for City business purposes and to increase the timeliness and effectiveness of City business communications.

1. At the discretion of an employee's Department Head, an employee may use City IT and equipment for private purposes, provided such use, including the value of the time spent, results in no incremental cost to the City or results in an incremental cost that is so small as to make accounting for it unreasonable or administratively impractical.
2. Employees are expected to use IT and equipment safely, responsibly, and primarily for work-related purposes. While employees may make personal use of City IT and equipment during working hours, the amount of use is expected to be limited to incidental use or emergency situations. Excessive time spent on such personal activities during working hours will subject the employee to disciplinary action.
3. Department Heads and Supervisors responsible for the evaluation and direct supervision of employees and are responsible for ensuring the appropriate use of all IT and equipment through training, supervising, coaching, and/or disciplinary action, if necessary. Department Heads and Supervisors may not ask for or maintain a list of employee's passwords or personal identification numbers ("PIN"). Access to employee files can be given by the IT Department as needed.
4. All employees share in the responsibility to protect City computer resources from physical and environmental damage and are responsible for the correct operation, security, and maintenance of those computer resources.
5. All employees have a responsibility to read and be familiar with the City's Employee Handbook that governs and guides City employee behavior.
6. All application data, documents, emails, files, programs, software, and any other electronic information stored on any computer system owned by the City is City property. This includes programs licensed by the City for its use. Such City property is subject to inspection for purposes of determining compliance with this and other City policies.

Employees are required to disclose passwords or other security devices upon request to the IT Department.

7. Software may be loaded and installed onto City computers only if its use has been approved and authorized by the IT Department and licensed by the City. All original license documentation and installation media will be turned over to the IT Department.
8. Software may not be copied from City computers for personal use. Unauthorized copying constitutes theft. If an employee has a need for software copies to work at home, the employee should consult the employee's Supervisor. If the City buys such software, it becomes City property and must be surrendered to the City upon request or at the end of the use or job. If an employee purchases software, all data remains the property of the City.
9. Data access by an employee is permitted only to the extent that the employee has been authorized. Even though additional data may be accessible by an employee, it does not mean that an employee has permission to access the same.
10. Employees should only use licensed versions of copyrighted software in compliance with vendor license requirements. Any unlicensed software should be reported to the IT Department immediately.
11. Employees should be considerate in the use of shared resources. Employees should refrain from monopolizing systems, overloading networks with excessive data, degrading services, wasting computer time, connect time, disk space, printer paper, manuals, and/or other resources.
12. Network drives are protected from unauthorized use by passwords. Setting private passwords on documents is not acceptable and should be removed if the document is stored on the network.
13. Data should only be stored on the users' drives or department drives. Data should never be stored on an end user's computer.
14. Regularly delete unneeded files and information from your accounts (if not required to retain the files as determined by policy or records management schedules).
15. Secure unattended computers (e.g., log off, lock, or otherwise make inaccessible), even if you will only be away from the computer for a moment. Do not override network lockout policies. Under no circumstance is any employee allowed to store access/passphrase information in plain sight or in an unsecure area.
16. Individual user identification and passwords are initially provided by the IT Department at the request of Division or Department Heads to employees to provide for appropriate access to accomplish job functions. Employees may change their own passwords by following a procedure specified by the IT Department.
17. The IT Department must be notified of any changes in personnel status of persons with user identification.

INAPPROPRIATE USE

Inappropriate uses of City IT and equipment includes, but is not limited to, the following:

1. Use of another employee's data, files, and/or systems without permission. NEVER allow another user to use your computer or any other computer with your login credentials.
2. Use of computer programs to decode passwords or access control information.
3. Attempts to bypass or deactivate system or network security measures. This includes using proxies to bypass the firewall or other content restrictions and/or controls put in place by the City.

4. Engaging in any activity that might be harmful to systems or to any information stored thereon, such as willfully or knowingly creating or propagating viruses, disrupting services, damaging files, or making unauthorized modifications to City data.
5. Use of IT and equipment for commercial, non-City related purposes which use could result in personal gain for an employee. Examples would include, but not be limited to, use of City IT and equipment to:
   i) solicit and communicate with customers;
   ii) prepare and distribute advertising and product information;
   iii) keep financial records of personal business activities;
   iv) sell products or services directly to customers; and/or
   v) create a product or service.
6. Making or using illegal copies of copyrighted materials or software, storing such copies on City systems, or transmitting them over City networks.
7. Use of email or messaging services to harass or intimidate another person, such as by broadcasting unsolicited messages, by repeatedly sending unwanted mail, or by using another person's name, email address, or user identification.
8. Displaying, disseminating, downloading, printing, receiving, sending, and/or viewing material that is defamatory, disruptive, fraudulent, harassing, illegal, intimidating, obscene, pornographic, sexually explicit, and/or slanderous. Such uses include, but are not limited to, the use of the intranet or internet to:
   i) send or forward email chain letters (usually determined by its request to send to other users) or pyramid-selling schemes, hoaxes, jokes, or urban legends; and/or
   ii) "spam," meaning exploiting list servers or similar broadcast systems for purposes beyond their intended scope in order to amplify the widespread distribution of unsolicited email (electronic junk mail or junk newsgroup postings).
9. Wasting computer resources or network resources, for example, by intentionally placing a program in an endless loop, printing excessive amounts of paper, storage of music files, listening and/or viewing of streaming media defined as video and audio feeds from the internet (the City Library and its employees are exempt from the streaming policy) or any other type of data not related to City business on the City's network, or by sending chain letters or unsolicited mass mailings as defined in section 8 above.
10. Selling access to a user identification or to resources on City systems or networks.
11. Use of IT and/or equipment for betting, selling, and/or wagering chances.
12. User identification and passwords shall not be disclosed, posted, or shared. IT personnel may take any appropriate action to insure sufficient security for computer systems and data. Passwords may be disclosed to IT personnel for IT purposes, with approval of IT Manager/Director.
13. Unauthorized deletion of any data, information, programs, and/or software from any computer or computer media is a violation of this policy.

C. ELECTRONIC COMMUNICATIONS POLICY

The City's email system is a tool for internal and external communications; the system is paid for and maintained by the City. Be advised of the following which applies to all employees using computers to access City owned networks, mail systems etc.:

1. The password assigned to or decided by you does not protect such communications or imply a right to personal privacy. There is no expectation of privacy.

2. The City can bypass your password.
3. Do not expect that your email messages will remain private.
4. To protect and comply with various State and Federal laws, the City reserves the right to periodically audit, disclose, monitor, review, and/or retrieve email communications sent and/or received on the City server at any time, without notice to employees. Employees should not assume that deleting emails erases email communications permanently from the City's system. Employees should learn and comply with the City's records retention system for email communications.

TRANSMITTING CONFIDENTIAL OR PRIVATE INFORMATION

The security or privacy of messages cannot be guaranteed on internet email systems. Data considered private or confidential should never be transmitted via internet email.

CONNECTION TO THE CITY NETWORK

1. No device may be connected to the City network either directly or indirectly without the permission of the IT Department. Equipment should only be installed, moved, or replaced by IT personnel unless prior permission is obtained.
2. All wireless access points must be disabled on any device that connects to the network.
3. Devices that host dynamic host configuration protocol are prohibited on the network.

PASSWORD/PASSPHRASE

1. Employees are responsible for protecting their user accounts and systems from unauthorized use.
2. Employees are responsible for all activities on their user accounts.
3. Care should be taken to protect the user account by choosing proper and secure passwords, changing the password when prompted, and not posting the password in written form in an accessible or viewable place.
4. Emailing of passwords is prohibited unless specified by the IT Manager or IT Director.
5. Do not leave your computer unattended without first locking or logging off (CRTL + L).
6. Immediately notify the IT Department if you believe your account credentials (i.e., user identification, password, passphrase, pin, etc.) have been compromised.

CAREFUL USAGE

Employee use of IT and equipment must be able to withstand public scrutiny from the City's taxpayers, employees, and vendors, among others.

1. Employees should use generally accepted standards of business conversation in all internet usage.
2. Employees shall exercise good judgment in the type of message created and the tone and content of messages.
3. The content of messages is always considered personal opinion unless specifically stated as a City position.

PARTICIPATION IN ELECTRONIC DISCUSSION GROUPS

Each employee's internet email address (username@meridenct.gov) clearly identifies the City. Thus, it is imperative that employees not participate in chat groups, emailing, instant messaging, news groups, and/or web-based discussion boards, where the content is not clearly related to City business. Such messages might be construed as an official City position.

INSTANT MESSAGING

The use of instant messaging programs is not allowed. The use of instant messaging programs compromises network security and degrades network performance. City owned and operated internal instant messaging programs are exempt from this rule.

MONITORING IT AND EQUIPMENT

IT and equipment are City property and are intended for City business.

1. The City reserves the right to monitor an employee's use of IT and equipment at the time of use, during routine post-use audits, and/or during investigations.
2. The City reserves the right to restrict an employee's access to various internet sites and services.
3. The actual content of email, internet access records, etc., is not routinely monitored or disclosed. However, employees should understand that email and voicemail messages, internet access records, etc., may be logged, retrieved, and reviewed by a Supervisory authority at a later date.
4. All internet and email activity can be viewed in real-time by IT staff and Department Heads at any given time.

DOWNLOADING/ATTACHING SOFTWARE

Unless authorized by the IT Department, employees may not install software downloaded from the internet, received on a disk, or received as an attachment to an email message. Receiving software in this manner presents a significant risk of computer virus infection.

1. Websites that require you to agree to a plugin in order to view the content should only be used if the plugin was preinstalled or approved of by the IT Department.
2. If installation of downloaded or attached software is authorized, employees must follow City policies for virus scanning.
3. NEVER install or open a file that you were not specifically expecting to receive. This includes Office documents, e-cards, images, and/or screensavers.

MAINTENANCE OF USER ACCOUNTS
ONBOARDING/OFFBOARDING PROCESS

It is the responsibility of Department Heads and Supervisors to inform the IT Department when an employee's account is no longer needed (i.e., when an employee ceases employment with the City, a temporary employee or intern leaves, or any account set up for special projects or installs is no longer needed). Leaving unused accounts active poses a security risk to the entire network.

1. Requests for adding user accounts, access to additional programs or software, access to another employee's files or data, or removing access to files, data, programs, or software must be made to the IT Department in writing by the employee's Department Head.
2. Onboarding and offboarding of any new or existing employees must be notified to Human Resources ("HR") and the IT department as soon as possible. HR will provide the proper forms for Department Heads to fill out. Forms will request the necessary equipment and user access for the new employee to perform job related tasks. This will keep as a record for equipment that is to be returned during the HR offboarding process and access that is to be terminated during an offboarding process. These forms will be used by IT to prepare new user accounts/access and equipment. It is a requirement to submit the information to HR for IT to prepare for the new employee.

DRIVE SHARING PROGRAMS

The use of any drive sharing or file sharing programs such as BitTorrent, Kazaa, Napster, WinMX, and/or any other program that sets up a peer-to-peer network over the internet is strictly prohibited. The use of such programs opens the City's network to the internet and is considered a breach of security.

VIRUS PROTECTION

Any computer that attaches to the City's network or shares data with any computer attached to the City's network must have standard virus scanning software installed and current virus signatures installed.

1. All files and programs must be scanned for viruses before being copied to any City information system.
2. Current virus signatures are distributed during the network login process; employees must not cancel the virus signature distribution process.
3. Upon notification of a virus, employees must contact the IT Department as soon as possible.
4. Under no circumstance is it acceptable for an end user to disable anti-virus software.
5. Alarms regarding known viruses shall be forwarded to the IT Department. Never forward a suspected virus.
6. Users may not take it upon themselves to alert the general user community. This will prevent hoax warnings from being disseminated.

D. USE OF MOBILE DEVICES

Cellular phones, laptops, personal digital assistants, smart devices, smartphones, tablets, USB drives, and other mobile devices are subject to the same policies and procedures as any other computer in respect to monitoring, examination of public records, installation of software, virus protection, and appropriate use.

1. When using a City owned mobile device, you must be clearly identified as a City employee while on the internet.
2. It is the mobile device user's responsibility to protect the computer from theft, unauthorized access, viruses, and extreme environmental conditions; all devices should be password protected.
3. Mobile devices should not contain confidential data that can compromise the personal data of residents or employees.
4. Mobile devices are not to be connected to home networks without prior approval from the IT Department and Department Heads.
5. The IT Department will determine the appropriate device to accomplish essential work related tasks.

REMOTE ACCESS

Programs that allow remote access to work computers are strictly prohibited without prior authorization from the IT Department. The City maintains a secure SSL VPN for users that may need remote access. Examples of prohibited programs include but are not limited to GoToMyPC, LogMeIn, Mikogo, and Teamviewer.

E. SOCIAL MEDIA POLICY

All City social media sites shall be:

1. Approved by the Social Media Administrator and the requesting Department's Head;
2. Published using the approved City social networking platform and tools; and
3. Administered by the Social Media Administrator or designee.
4. The official posting for the City will be accomplished by the Social Media Administrator and/or his/her designee.
5. All social networking sites shall clearly indicate that the sites are administered by the City and shall have City contact information prominently displayed.
6. City employees shall not administer unauthorized social media sites that contain the indicia of an official site, including the City's Official Seal or titles or statements which state, imply, or suggest that the site is an official City site.
7. City employees shall not administer unauthorized social media sites which purport to reflect the views of the City.
8. All City social networking sites shall adhere to applicable State, Federal, and local laws, regulations, and policies, including all IT and retention schedules, Freedom of Information Act management policies, and other applicable City policies.
9. Freedom of Information Act and e-discovery laws and policies apply to social media content, and, therefore, content must be able to be managed, stored, and retrieved to comply with such laws.

10. All social network sites, content, and entries shall clearly indicate that any articles and any other content posted or submitted are subject to public disclosure.
11. The City reserves the right to restrict or remove any content posted in an official capacity that is deemed in violation of this policy or any applicable law.
12. Each City social networking site shall include an introductory statement which clearly specifies that the site is an official City site as well as the purpose and topical scope of the blog and/or social network site. Where possible, social networking sites should link back to the official City website for forms, documents, and other information.
13. City social networking content posted as City business by any administrator or employee containing any of the following forms of content is not allowed for posting:
    i) Profane language or content as defined herein.
    ii) Content that promotes, fosters, or perpetuates discrimination on the basis of age, color, gender, gender identity, marital status, mental health disability, national origin, public assistance status, physical disability, race, religion, and/or sexual orientation.
    iii) Sexual content or links to sexual content.
    iv) Conduct or encouragement of illegal activity.
    v) Information that may tend to compromise the privacy, confidentiality, safety or security of the public or public systems.
    vi) Content that violates a legal ownership interest of any other party.
    vii) Political content in violation of Federal and/or State statutes.
14. All City social networking administrators shall be trained regarding the terms of this policy, including responsibilities to review content submitted for posting to ensure compliance with the policy.
15. Where appropriate, City IT security policies shall apply to all social networking sites and articles.
16. All City employees, including social network administrators, representing the City government via social media outlets must conduct themselves at all times as a representative of the City.
17. The City Social Media Administrator will maintain a list of usernames, passwords, and PINs for any social media site used.
18. Passwords should not be changed by the user without first notifying the Social Media Administrator.

F. ADDITIONAL GUIDELINES

1. Email tone and language is important. It is easy to misinterpret the meaning of a communication (i.e., caps as shouting, brief sentences as curt).
2. Reasonable personal use of email is acceptable; however, employees have no right to privacy, including the review of deleted messages.
3. Jokes, obscenities, pictures, and/or vulgarities that target race, sex, or other protected classes (i.e., age or disability) will not be tolerated by the City. The City's sexual harassment policies apply to employees' email communications. Unacceptable behavior in the workplace is also unacceptable in cyberspace.
4. Email senders should identify themselves and should not falsify their identity in any way.
5. Email should not be used for outside business ventures, political, or religious use. The City's Code of Ethics is always applicable.

CONFIDENTIALITY

Notwithstanding the City's right to retrieve and read any email messages such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees other than designated representatives are not authorized to retrieve or read email messages that are not sent to them. Any exception to this policy must receive prior approval from your Department Head.

DISCIPLINARY ACTION, SUSPENSION, TERMINATION, OR RESIGNATION OF AN EMPLOYEE

In cases where an employee is subject to disciplinary action, suspension, or termination, in compliance with bargaining unit contracts, or where an employee voluntarily resigns, access to IT and equipment may be limited or terminated. Department Heads are responsible for the integrity and control of equipment and the information systems to which their employees have access. It is the responsibility of the Department Head to notify the IT Department as soon as possible if an employee will be leaving a position to insure that access to IT and equipment can be terminated upon the employee's departure. Department Heads should notify the IT Department immediately if there is a need to limit an employee's use of any IT or equipment in cases of disciplinary action, suspension, or involuntary termination of an employee.

G. CONCLUSION

This *Acceptable Use Policy for Information Technology* is intended to ensure that the City's technology systems are used in an efficient and responsible manner. Failure to comply with any part of this *Policy* may result in appropriate discipline up to and including termination. If an employee is a member of any union or otherwise covered by a collective bargaining agreement with the City, such individual may exercise any and all rights prescribed by such agreement in accordance with any processes prescribed by such agreement. In addition, violations of this *Policy* may be reported to law enforcement agencies where appropriate. Employees who discover a violation of this policy or have other complaints should promptly notify the HR Department.

DRUG FREE WORKPLACE POLICY

Purpose

To comply with the requirements of the Federal Drug Free Workplace Act of 1988 (the "Act") and to establish a safe and healthy workplace that is drug and alcohol free. This policy serves as notification to all employees of the requirements of the Act and the City's ongoing, good-faith efforts to maintain a drug free workplace by meeting the requirements of the Act.

Definitions

Controlled Substances: Includes, but is not limited to, any narcotic drug, hallucinogenic substance, amphetamine, and marijuana among many others commonly thought of as illegal drugs, as well as certain medications if not taken under a physician's prescription or according to a physician's orders. Controlled substances are specifically defined in federal law, Schedules I – V of Section 202 of the Controlled Substance Act (21 U.S.C. § 812) and 21 C.F.R. §§ 1300.11 – 1300.15.

Application

Any individual who is employed by, who conducts business for the City or on the City's property, or is applying for a position with the City, must abide by this Policy. Employees covered by collective bargaining agreements may be subject to additional requirements in conjunctions with such agreements, such as drug testing.

Policy Statement

The unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance, whether the employee is on or off duty, in City workplaces, vehicles and City-owned residences, or while conducting City business off City worksites, is strictly prohibited. It is prohibited for any employee to be under the influence of a controlled substance, including alcohol and prescription drugs used inappropriately or not prescribed for him/her by a physician, while on the job or in the workplace. All employees are expected and required to report to work on time and in appropriate mental and physical condition for work. Violations of this policy will result in disciplinary action, up to and including termination. Violations may also have criminal consequences.

Notification Requirements

As mandated by the Act, employees, as a condition of employment, must abide by this Policy and must report any conviction under a criminal drug statute. This report must be made in writing within five (5) days after the conviction to the employee's Department Head and to the Director of Personnel.

Within 10 days of receipt of a report of a conviction, the City will notify any applicable federal granting/contracting agency of the violation. Such notice must include the convicted employee's position/title and the applicable grant or contract identification number.

Penalties for Violations

As a condition of employment, any employee who violates this Policy will be subject to discipline, up to and including termination, and/ or referred to a drug abuse assistance or rehabilitation program and required to demonstrate satisfactory participation in such program. Employees covered by a collective bargaining agreement will be disciplined in accordance with the terms of such agreement. The Act requires that appropriate personnel actions must be taken within 30 days of receipt of a report of a conviction.

Awareness Program/ Treatment Services

The City, in compliance with the Act and with the goal of maintaining a drug free environment, has established the following Drug Free Awareness Program to help make employees aware of the dangers of drug abuse and the available counseling, rehabilitation, and employee assistance programs.

a. Employees needing help in dealing with drug and/or alcohol dependency are encouraged to use the City's Employee Assistance Program ("EAP") and health insurance plans, as appropriate. Employees are encouraged to contact the City for more information on available programs and to obtain contact information for current providers.

b. The City will provide on-going training and education for employees through its EAP program. Such training and education will include information about available drug counseling and employee assistance programs.

Nepotism Policy

In situations where family members are supervised by each other it is important for supervisors to avoid even the appearance of impropriety. As in all supervisory situations favoritism, harassment, and any other inappropriate supervisory behavior cannot be tolerated.

In all situations where a family member is supervised by another family member, the department head or supervisor when issuing discipline or adjudicating a grievance shall meet with the Director of Personnel and follow any recommendation.

In situations where it would be inappropriate for the supervisor or department head to discipline someone, such a violations that may be cause for suspension or termination, another supervisor or the Director of Personnel shall act in their capacity at such meeting.

Any supervisor who enters into a romantic relationship or cohabitates with a subordinate must disclose such relationship within 30 days to the Director of Personnel.

At no time shall a Department Head make a decision to promote their family member without disclosing the relationship and getting approval from the Director of Personnel

In situations where a department head has discretion over appointments, they shall use such discretion in a way that does not cause family members to be supervised by each other.

Any complaints regarding nepotism should be immediately reported to the Director of Personnel or City Manager and will be promptly investigated.

Failure to follow the above rules may be cause for discipline up to and including termination

Family member / close relative is defined as spouse, child, parent, aunt, uncle, niece, nephew, brother, sister, son-in-law, daughter-in-law, first cousin, stepfather, stepmother, stepbrother, stepsister, stepchild, brother-in-law, sister-in-law, grandparents and grandchildren. Relationships include those through marriage and adoption.

SEXUAL HARASSMENT POLICY

SEXUAL HARASSMENT – It is the policy of the City of Meriden that sexual harassment in the Workplace is unacceptable and will not be tolerated. All employees/interns of the City of Meriden, whether management personnel or non-management personnel, are expected to avoid any behavior or conduct toward any other employee/intern that could be interpreted as sexual harassment

Sexual harassment is defined generally as "unwelcome sexual advances, requests for sexual favors and other verbal or physical conduct of a sexual nature". Thus, no employee/intern should be subjected to unsolicited and unwelcomed sexual overtures or conduct, either verbal or physical or be led to believe that an employment opportunity or benefit will in anyway depend upon "cooperation" of a sexual nature.

Sexual harassment may include such actions as: sex oriented verbal "kidding", "teasing", or jokes; Repeated offensive sexual flirtations, advances, or propositions; continued or repeated verbal abuse of sexual nature; graphic or degrading comments about an individual or his or her appearance; the display of sexually suggestive objects or pictures; subtle pressure for sexual activity; physical contact such as patting, pinching, or brushing against another's body; or demands for sexual favors

Conduct of this type is improper if:

a) Submission to the conduct is either an explicit or implicit term or condition of employment;
b) Submission to or rejection of the conduct is used as basis for employment decisions affecting the person involved;
c) The conduct has the purpose or effect of interfering with an individual's work performance or environment.

Sexual harassment does not refer to occasional compliments of a socially acceptable nature. It refers to behavior which is not welcome, which is personally intimidating, hostile, or offensive which debilitates morale, and therefore interferes with our work effectiveness.

Appropriate management and supervisory personnel shall promptly investigate all complaints of sexual harassment, including interviewing the complainant and the person (s) alleged to have engaged in sexual harassment. All involved parties should be spoken with privately to afford them the opportunity to voice any complaints or concerns. If, as a result of the investigation, it is found that the complaint has merit, the appropriate management and supervisory personnel shall take prompt corrective action.

Such actions may include discipline up to and including termination of the offending employees/ Intern(s).

Any employee/intern of the City of Meriden who feels that he or she has been the victim of sexual harassment should notify his or her supervisor, department head, Director of Personnel, or City Manager at the very earliest opportunity. If the complaint is found to have merit, corrective Disciplinary action will be implemented. If the complaint is found to be of insufficient merit, all involved parties will be so notified.

No Retaliation

Retaliatory action against an individual who files a complaint in good faith will not be tolerated and may subject an offending employee/intern to disciplinary action, up to and including termination of employment.

However, the City also recognizes that false accusations of harassment or their unlawful conduct can be damaging to an accused employee/intern and disruptive to our agency's operations; knowingly making false accusations may constitute misconduct for which disciplinary action may be imposed.

All employees/interns deserve equal treatment and to work in a pleasant, supportive environment.

If you are the victim of, or witness harassment, please call Deborah Moore, Human Rights Advocate, Caroline Beitman, Director of Human Resources or your department head and report the situation immediately and we will investigate and if necessary, issue corrective action. Also you can contact Connecticut commission on Human Rights & Opportunities at the numbers listed below.

Deborah Moore – Human Rights Advocate (203) 630-4045
Caroline Beitman – Director of Human Resources (203) 630-4037

Connecticut Commission on Human rights & Opportunities

West Central Region, 55 West Main Street, Suite 210, Waterbury, CT 06702-2004
(203) 805-6579

Capitol Region, 1229 Albany Ave, Hartford, CT 06112 (860) 566-7710

TOBACCO USE

The City recognizes the serious health risks associated with the use of all tobacco products and E-cigarettes. Thus, the purpose of this policy is to promote a healthy work environment. The following provisions will apply to the use of all tobacco products and E-cigarettes:

- No tobacco or e-cigarette use in city vehicles
- No tobacco or e-cigarette use in city buildings
- No tobacco use on city time (except breaks / lunch)
- The use of tobacco products is permitted exclusively in areas customarily designated for smoking.
- The use of tobacco products in these areas is permitted during lunch breaks and specified union breaks only.
- Employees must properly dispose of all waste products associated with use of any tobacco product.
- Failure to adhere by these guidelines will result in disciplinary action.

The City periodically provides assistance to any employee who would like to receive treatment for tobacco addiction. Please contact the City of Meriden Department of Health and Human Services for more information.

WORKPLACE VIOLENCE POLICY STATEMENT

It is the City of Meriden's policy to promote a safe working environment for its employees. However, the City of Meriden recognizes that violence is a growing problem in the workplace. The City of Meriden is committed to working with its employees to maintain a work environment free from violence, threats of violence, harassment, intimidation and other disruptive behavior. While this kind of conduct is not pervasive in the City of Meriden, no employer is immune. Every employer will be affected by disruptive behavior at one time or another.

Any violence, threats, intimidation and other disruptive behavior in our work place will not be tolerated; that means, all reports of incidents will be taken seriously and will be dealt with appropriately. Such behavior can include oral or written statements, gestures, or expressions that cause physical harm or bodily injury to any employee of the City of Meriden. Such behavior is unacceptable and individuals who commit such acts maybe removed from the premises and maybe subject to disciplinary action, criminal penalties or both.

In accordance with this policy, except as required as a condition of employment, no employee shall bring to any City worksite any weapon or dangerous instrument. Weapon is defined as a firearm, including a BB gun, whether loaded or unloaded, any knife, switch blade with or without an automatic spring release device, a stiletto or martial arts weapon. Dangerous instrument means any instrument, article or substance that, under the circumstances, is capable of causing death or serious physical injury.

The City of Meriden is committed to a policy of zero tolerance for incidents of workplace violence. Therefore, any employee found engaging in any such conduct or possessing any weapon or dangerous instrument at any City worksite will be subject to termination in accordance with Union contracts.

We need your cooperation to implement this policy effectively and maintain a safe working environment. Do not ignore violent, threatening, harassing and intimidating or other disruptive behavior. If you observe or experience such behavior by anyone at the City of Meriden, whether he or she is a City of Meriden Employee or not, report it immediately to a supervisor or manager. Supervising managers who receive such reports should seek advice from Caroline Beitman, Director of Human Resources, regarding investigating the incident and seek appropriate action.

(PLEASE NOTE: THREATS OR ASSAULTS THAT REQUIRE IMMEDIATE ATTENTION BY SECURITY OR POLICE SHOULD BE REPORTED FIRST TO THE POLICE AT 911).