COLLINS, LOUGHRAN & PELOQUIN, P.C.
Attorneys at Law
320 Norwood Park South
Norwood, Massachusetts 02062

Tel. (781) 762-2229 • Fax (781) 762-1803
www.collinslabor.com

Philip Collins
Leo J. Peloquin
Tim D. Norris
Joshua R. Coleman
Melissa R. Murray

Employer Rights and Obligations When Monitoring Employees at Work

A Presentation to the
Massachusetts Municipal Association
Annual Meeting

January 22, 2016
by
Leo J. Peloquin, Esq.*
Collins, Loughran & Peloquin, P.C.
320 Norwood Park South
Norwood, MA 02062
(781) 762-2229

NOTICE: This handout does not purport to give legal advice for any specific situation, or, come to think of it, even a general situation.

*The presenter was assisted in preparing these materials by Attorneys Philip Collins, Melissa R. Murray, Joshua R. Coleman and Law Clerk Jennifer King.

For more detail on DLR cases, please see our firm's Management Commentary in Landlaw's publication of their cases.

I. USE OF EMPLOYER TECHNOLOGY

A. What To Cover Under An Acceptable Use Policy

- Employer devices: computers, computer files, computer network, email systems, Internet access, telephones, cell phones, smartphones, tablets, cameras, recording devices

B. Why Have A Written "Acceptable Use" Policy

- Productivity: Devices belong to Employer, provided for work, not personal use, and subject to being monitored by Employer.
- Establish limitations on personal use.
- Monitor and prevent activity that generates employee claims like discrimination, harassment, defamation, hostile work environment.
- Dispel any employee expectation of privacy.
- Prevent employees from transmitting confidential, proprietary.
- Damage to devices and systems.
- Notice to employees of consequences for violations.

C. Union Use Of Employer Email

- Can't restrict Unions from using Employer email during non-work time for discussions among employees about terms and conditions of employment. Purple Communications, Inc., 361 NLRB 126 (2014).
- Purple Communications, Inc. overturned law that said, because email system was Employer's property, Employer could ban all non-business e-mail communications. No ban allowed unless Employer satisfies the heavy burden of showing that special circumstances make restrictions necessary to maintain production and discipline.
- Rationale: A recognition that e-mail "is the predominant means of employee-to-employee communication" and workplace communication is the foundation of protected concerted activity.
- **Massachusetts ahead of its time for Unions.** DLR finds that Employer violated c. 150E (illegally coercive) when it threatened ban on use of Police Department's email for anything but police business because union member

disseminated an email complaining about a recent meeting with management. Hearing Officer ruled that email in question was protected concerted activity. Department had previously allowed union members to send non-business emails, ranging from union business to exchanging jokes. City of Northampton v. Local 590, IBPO, 21 MLC 1390 (1994).

II. CELLPHONES: Restricting Use; Employer Searches

- No obligation to bargain when Department instituted a policy prohibiting jail officers from using private cell phones on the job because Department's interest in ensuring that jail officers are able to provide for the care, custody and control of inmates without distraction is a managerial right and outweighed the employees' interests in carrying their cell phones. Suffolk County Sheriff's Department, 29 MLC 63 (2002).

- Must bargain policy that not only prohibits cell phone use while operating Town vehicles or equipment, but disallows the possession or use of cameras/camera phones in the workplace without specific authorization, limits the use of Town-issued phones for personal business, and limits the making or taking of personal calls at work. Town of Plymouth, 40 MLC 65, aff'd 40 MLC 2009 (2014) (CERB declines to "parse out" safety component).

- Use policy to dispel any expectation of privacy

III. GPS DEVICES

- M.G.L. c. 150E Employer "Unilateral" Right To Use New "Technology": An Employer can alter a procedural mechanism for enforcing existing work rules without bargaining, provided that the Employer's actions do not change underlying conditions of employment.

- But Commonwealth Employment Relations Board ("CERB") upholds Hearing Officer decision that overturned precedent of no bargaining obligation with GPS technology because no change in standards of productivity and performance. ("The increased monitoring of, and information about, employee job performance and productivity affected employees' underlying terms and conditions of employment such that the City was required to bargain over whether to install the devices and whether and how it intended to use the constant stream of information before installing them.")Springfield v. American Federation of State County and Municipal Employees, 41 MLC 130, aff'd 41 MLC 383 (June 30, 2015).

- CERB Rationale:

- "The clandestine installation of devices that enable an employer, for the first time, to engage in constant, remote electronic monitoring of aspects of employee performance that had not been previously routinely reported or observed plainly constitutes the institution of a new practice."

- Even if no new work standards were created, the devices greatly increased the amount of data that the City had to evaluate work performance and productivity. It noted that, within four days of the installation of GPS devices, the City notified a union official that it had monitored and recorded two unauthorized trips to conduct union business. "The increased monitoring of, and information about, employee job performance and productivity affected employees' underlying terms and conditions of employment such that the City was required to bargain over whether to install the devices and whether and how it intended to use the constant stream of information before installing them."

- City has appealed to the Appeals Court. Is DLR/CERB wrong? The City has always required DPW workers to report to work at their assigned location and perform their assigned job. The act of installing and monitoring a GPS device has not imposed a reporting requirement on its employees, as employees are not required to make a "report" regarding their daily tasks. Finally, even in cases where employees were unaware of the GPS device's presence, working conditions were not changed because in years prior to GPS, supervisors could randomly check on an employee's work without providing the employee with prior notice. Just because new technology is better, it has to be bargained?

  - Police Cruiser GPS: Does public policy outweigh bargaining obligation?

IV. VIDEO SURVEILLANCE OF EMPLOYEES

A. Plan on Bargaining

1. Employer's right to install surveillance cameras to ferret out time sheet falsification did not have to be bargained "[b]ecause the use of the surveillance was limited to recording the custodians' departure times and was in response to a specific concern about the accuracy of the existing method of timekeeping… [it was].merely a more efficient and dependable means of enforcing existing work rules and did not affect an underlying term [of employment]." Duxbury School Committee, 25 MLC 22 (1998).

2. City's installation of a time clock and video surveillance of the clock as a better means of documenting employee work hours had to be bargained before implementation because it was a "new, changed, more stringent practice."

Previously, employees either reported their arrival times and absences to a supervisor or filled out a Daily Attendance Sheet. City of Taunton, 38 MLC 96 (2011).

V. BODY WORN CAMERAS

- The ultimate surveillance of employees forms the new battleground.

A FINAL EXAM

1. In the wake of an accident in a Town vehicle which was reportedly caused by the driver checking his phone, the Town Administrator announces that all employees who drive Town vehicles will not be allowed to carry their cell phones with them during the work day. The Union files a "unilateral change/failure to bargain" charge at the Department of Labor Relations.

    1. Was there a more defensible approach for the Town Administrator to take?
    2. What is the Town's best argument?
    3. What is the Union's best argument?
    4. How will the case come out?

2. The City Manager discovers that Union members are using the Town's email system during their working hours to disseminate alleged violations by Management of the parties' collective bargaining agreement and even to circulate potential proposals during successor Contract negotiations. The City Manager disseminates a directive to all City employees that bars the use of the City's email/computer system for any purpose other than their work duties and that employees will face discipline, up to and including dismissal for doing so. The Union files a "unilateral change/failure to bargain/coercion" charge.

    1. Was there a more defensible approach for the City Manager to take?
    2. What is the Union's best argument at the DLR?
    3. What is the City's best argument?
    4. How will the case come out?

3. The Town has historically monitored the locations of DPW employees doing snow removal through intermittent radio communications and live checks by on the road supervisors. The Town installs GPS devices in the equipment. Relying on the GPS data, the Town disciplines a driver for spending too much time on a break. The Union files a unilateral change/failure to bargain charge at the Department of Labor Relations.

    1. Was there a more defensible approach for the Town to take?
    2. What is the Town's best argument?
    3. What is the Union's best argument?
    4. How will the case come out?

4. The City discovers that the cash in the cash box in the Recreation Department does not match the receipts provided to customers. The City is able to narrow down the dates that money is taken to two employees (A and B). The decision is made to secretly install video cameras in the office where the money is kept and activate them on the days A and B are working. Lo and behold, the cameras pick up employee A pocketing money. The City fires employee A. The Union files a grievance as well as a "unilateral change/failure to bargain" charge at the

DLR, including that the City was obligated to bargain over the secret installation of the camera, the evidence gathered from the unilateral change cannot be used against the employee and the dismissal must be overturned.

1. What would be helpful information to know from the City in defending its actions?
2. What is the City's best argument at the DLR?
3. What is the Union's best argument at the DLR?
4. Who wins?

5. The City is so pleased about how the video cameras worked in discovering the stealing clerk that they decide to openly install them in all City offices where money is handled. The Union files a "unilateral change/failure to bargain" charge.

    1. What is the City's best argument at the DLR?
    2. What is the Union's best argument at the DLR?
    3. Who wins?

6. Jane and Dan have held non-union administrative positions with the Town for several years. Despite an email policy against it, they routinely obtain and disseminate to co-workers sexually explicit e-mails from internet joke sites and other third parties, including their respective spouses. One day, however, an employee complains to management about the content of an e-mail the employee received. The Town's IT person goes into the email of Jane and Dan and finds the evidence that they are the primary disseminators of the offensive material. Jane and Dan are e fired for violating the Employer's e-mail policy. Jane and Dan sue the Town for invasion of privacy, violation of the Massachusetts Wiretap Statute and violation of public policy. Their main argument is that the e-mail received and sent was personal.

    1. What would be helpful information to know from the City in defending its actions?
    2. What is the Town's best argument?
    3. What is the Plaintiffs' best argument?
    4. Who wins?
    5. How would the case come out if there was no email policy?

SAMPLE POLICIES/CONTRACT PROVISIONS

1. Less Said Is Not Better For The Employer

a. DLR Standard. Employer's burden to prove that the negotiated provision "clearly, unequivocally and specifically authorizes its actions."

b. Management Rights Language That Sounds Tough But Doesn't Give Managements. Unless clearly and specifically relinquished, abridged, or limited by this Agreement, the Employer, through its Town Manager, Board of Selectmen and/or other appropriate officials as may be authorized or designated to act on its behalf, retains all the rights and prerogatives of municipal management established either by law, custom, practice and precedent.

2. Management Right To Investigate: Management has the right to investigate employees for conduct that that violates their employment obligations and to use any and all technology and methods to do so, including surveillance of any type.

3. GPS Policy

- The Employer, in its sole discretion, has the right to implement Global Positioning System (GPS) technology, on any and all Town owned vehicles and to promulgate such policies as it deems necessary related to the use of said technology. This shall include the right to use this technology for any purpose, including monitoring employees' location, activities and performance and disciplining employees.

4. Cell Phone Policy

Cellular phones shall include smart phones. Town provided cellular phones are for business purposes only, unless otherwise authorized by the department head. They are to be used for non-work related communications only in exigent circumstances. Unless otherwise expressly authorized, employees may only use personal cell phones for an emergency.

In addition to telephone service, many cell phones or cellular providers offer a host of additional functions and/or services, including text messaging and digital photography. It is not possible to list all of the services that are now -- or may become -- available. Whether enumerated or not, employees are strictly prohibited from using any of these services while at work unless it is for a work purpose.

The use of a cell phone while at work may present a hazard or distraction to the user and/or co-employees. This policy is meant to ensure that cell phone use while at work is both safe and does not disrupt business operations. The intent of the policy is to enhance safe working conditions for employees and the general public by prohibiting

the use of cell phones while operating any motor vehicle on duty, which is a serious safety violation. Employees are reminded of their obligation to obey all applicable state and federal motor vehicle safety laws. A moment of inattention can produce tragic results.

Town issued cell phones are subject to being returned to the Town and searched at any time at the request of the Town. Personal cell phones are subject to being searched at any time at the request of the Town provided the Town has a reason to believe that their use was in violation of this policy.

Violations of this policy will be subject to disciplinary action, up to and including termination of employment.

5. Acceptable Use Policy

1.0 Technology Use Policy

The Town of [INSERT] ("Town") provides technology in order to allow Town of [INSERT] government to serve the public more efficiently and effectively. This policy is intended to provide rules and guidelines concerning the appropriate use of the Town's technology resources. Any person using the Town's technology shall be considered a user ("user") for purposes of this policy.

The term, technology, covers a wide range of processes used for communicating information within our society. Computers form one element of this broad term, but it also includes cellphones and smartphones, telephones, tablets, cameras and recording devices, video resources and various social media outlets and tools. Town computers, computer files, e-mail systems, Internet access, telephones, cellphones and smartphones, software and/or other technology furnished to town employees are the property of the Town of [INSERT]. All technology provided by the Town is intended for Town business. Employees may use the Internet service provided by the Town during their non-working hours, provided they adhere to all of the following regulations. All information and communication on Town equipment is considered Town/Public information and may be viewed at any time by management.

The users of the Town's network are responsible for respecting and adhering to local, state, federal and international laws. Any attempt to break those laws through the use of the network may result in litigation against the offender by the proper authorities and where appropriate, disciplinary action.

To the extent an employee uses his/her personal device to create Town records, those records must be transferred to the Town network/system as soon as possible. Employees who use their own personal technology device(s) to conduct Town business must provide the Town with access to these records and/or device(s) should the need arise.

1.1 User Responsibilities

This policy applies to every employee, board member (elected or appointed), contractor or remote user who is provided access to the Town's technology resources. It is the responsibility of any person using the Town's technology to read, understand and follow this policy. In addition, users are expected to exercise reasonable judgment in interpreting this policy and in making decisions about the use of information technology recourses. Any unauthorized, deliberate action, which damages or disrupts a computing system, alters its normal performance, or causes it to malfunction, is a violation, regardless of the system location or time duration.

1.2 Unacceptable Uses

This Policy sets forth general guidelines and examples of prohibited uses of the Town's technology, but does not attempt to identify all required or prohibited activities by users. Questions regarding whether a particular activity or use is acceptable should be directed to a supervisor, Network or Systems Administrator and/or Human Resources. Unless such use is reasonably related to a user's job and with their manager's approval, the following technology and computer-related activities are among those uses which are prohibited:

1.2.1 Illegal duplication of software or violation of copyright law by the duplication or sharing of software, or the distribution of copyrighted materials.

1.2.2 **Installation Of Unauthorized Software**. Software that is not purchased/licensed by the Town is considered unauthorized.

1.2.3 Intentional attempts to "crash" network systems or programs.

1.2.4 Attempts to use a password, access a file, or retrieve a stored communication that is not normally accessible to the employee/individual.

1.2.5 The willful introduction of computer "viruses" or other disruptive/destructive programs into the Town's network or into external networks.

1.2.6 Use of abusive or objectionable language or content in either public or private messages.

1.2.7 Activities that are libelous and/or amount to sexual, racial or other forms of harassment.

1.2.8 Using a Town e-mail address when posting to public forums, e.g. blogs, social media websites, wikis and discussion boards for personal use.

1.2.9 Accessing social networking sites for personal use during work hours.

1.2.10 Use of cameras or digital/audio recording devices to capture or record content without the permission or knowledge of the subject(s) being recorded.

1.2.11 Creating and/or distributing to members of the public, non-public information without proper authorization and, where necessary, proper protection.

1.2.12 Use of systems and/or networks in attempt to gain unauthorized access to remote systems or to connect to other systems, in violation of the physical limitations of the local/remote system.

1.2.13 Unauthorized Use of Network "Sniffers" or Other Network Analysis Tools.

1.2.14 Decryption of System or User Passwords.

1.2.15 The Copying of System Files.

1.3 Exception For Legitimate Business Reason

If any of the above prohibited uses is required for a legitimate business reason, an exception may be requested in writing to management. Management will review the request and grant an exception at its discretion.

1.4 Internet Access And Use

Internet access through the Town-provided network is intended for business use, including finding vendor information, government information, research, and communicating with colleagues and residents for government-related purposes. All internet usage will be monitored.

The Town grants users the privilege of Internet access for limited personal use, such as looking at home pages and sending e-mails to friends. This privilege of personal use of the Internet is subject to the terms and conditions established by the Town herein, and at the discretion of Town management, they may be amended from time to time and the privilege may be withdrawn in the future, with or without cause. Personal use of the Internet must be on the employee's own time.

Town owned technology resources may be used for personal purposes on a limited basis, providing the following requirements are met:

a. No marginal cost to the Town.
b. No interference with work responsibilities.
c. No disruption to the workplace.

At no time may the Internet be used for any type of commercial use, or to transact non-governmental business. The use of the Internet to solicit or recruit others for commercial ventures, religious or political causes or outside organizations or for personal gain is prohibited.

At no time may users access inappropriate websites, such as those hosting pornography, obscene materials or gambling enterprises.

The use of any element of the Town's computer system, including Internet access, for the receipt or transmission of information disparaging to others based on race, national origin, sex, sexual orientation, age, disability, or religion is not permitted under any circumstances.

Users are not permitted to download executable files from the Internet unless previously approved by the network administrator.

1.5 Electronic Mail (E-Mail) Access And Use

E-mail is an effective tool for sharing and disseminating information. The Town's e-mail system is linked to Internet systems, which allows users to communicate with other Town employees, colleagues in state agencies, vendors and residents. This electronic communication promotes better information exchange between Town employees and residents.

As with all of the Town's assets, the e-mail system is intended to be used for work-related purposes, and in ways consistent with the Town's overall policies. The system may not be used in any way that is disruptive to the operation of the Town or offensive to others. E-mail and Internet access should be used in a way that all transmissions, whether internal or external are accurate, appropriate, ethical and lawful.

The use of e-mail for the transmission of information that is harassing or disparaging to others based on race, national origin, sex, sexual orientation, age, disability or religion is not permitted under any circumstances. Likewise, e-mail is not to be used to solicit or recruit others for commercial ventures, religious or political causes or outside organizations, or personal gain, including, but not limited to, "chain letters" and/or requests for private donations.

The use of broadcast e-mail (sending the same message to a group of employees) places stress on the e-mail system and has the potential for generating undesirable volumes of junk mail or spam. Therefore, it should be used selectively for only work-related reasons.

Confidential information should never be transmitted or forwarded to outside entities or individuals not authorized to receive such information, or to Town employees having no business reason for having/receiving such information.

All e-mail sent or received using Town equipment is considered Town information/property and is subject to monitoring at the discretion of Town Management. The Town does not ensure the privacy and confidentiality of e-mail transmissions. While an employee's Town provided e-mail account may require a password for access, the employee should maintain no expectation of privacy in this account or in messages communicated through this account. E-mail transmissions may be subject to disclosure through legal proceedings or otherwise through various laws which

may be held to apply to such transmissions. E-mail messages and other use of the Town's computers may be considered to be public records, subject to disclosure under the public records law, depending on the contents of the communication or file.

2.0 Social Media Policy

The Town of [INSERT NAME] depends on a respectful work environment to achieve its goal of serving the residents of [INSERT NAME]. While social media can be a fun way to share one's life and opinions with others, its use presents certain risks and carries with it certain responsibilities. To assist employees in making responsible decisions about the use of social media, the Town has established these guidelines for appropriate use of social media.

The purpose of this policy is to help ensure that the social media activities of Town employees, conducted in both their official and personal capacity, conform to applicable laws, industry guidance, legal and regulatory restrictions, and privacy and confidentiality requirements. This Policy shall be read and interpreted in conjunction with all other Town policies and procedures.

This policy is designed to promote appropriate social media use and avoid uses that: (1) breach confidentiality by revealing protected information about the Town, its residents, or its employees; (2) expose the Town to legal liability for employer or employee behavior that may be harassing, offensive, or maliciously false; or (3) interfere with employees' productivity and their ability to perform the duties and responsibilities of their positions with the Town.

2.1 Scope

This policy applies to all Town employees, board members (elected or appointed), contractors, agents or remote users, while at work or away from work, engaging or causing others to engage in social media. To the extent that laws and regulations' applicability are unclear, Town management will make reasonable judgments regarding applying existing print rules to social media forums, and will conform to prevailing industry practices to the greatest extent possible and in all events to the requirements of law.

Town personnel working with third parties are responsible for assuring that such third parties are properly trained on this policy, and for monitoring their activities to ensure the third parties adhere to this policy.

This policy shall in no respect apply to preclude, impair or limit the right or ability of Town employees under M.G.L. c. 150E to communicate about terms and conditions of employment, and issues directly related thereto.

2.2 Definitions

Social Media: All forms of electronic communication, including online forums where users communicate or post information or content of any sort, including web logs, blogs, personal websites, journals or diaries, social networking or affinity websites, web bulletin boards or chat rooms, and file sharing sites. Social media does not include static web-based media that does not facilitate collaborative information sharing or user-generated content, such as websites that do not allow for user comments or content contributions.

Examples of social media include, but are not limited to, Facebook, Twitter, LinkedIn, MySpace, Google Plus+, youTube, Snapchat, Pinterest, Meetup, Friendster, RSS feeds, Classmates.com, Match.com, and Instagram.

Social Network: An online social structure or forum of friends, colleagues, acquaintances, and other personal contacts where users create profiles to share information and socialize with others.

Blog: A self-published diary or commentary on a particular topic that may allow readers to post responses, reactions or comments.

Page: The portion of a social media website where content is displayed and managed by an individual or group of individuals with administrator rights.

Post: Content an individual shares or publishes on a social media site or page. A post may also be referred to as a Comment.

Profile: Information that a user provides about him or herself on a social networking website.

Speech: Expression or communication of thoughts, opinions, or ideas in spoken or written form, through expressive conduct, photographs, video, symbolism, or other related forms of communication.

Tagging: Externally visible demarcations published by users that are used to identify content by associating it with a keyword.

Tweet: A post or status update on Twitter.

Users: Employees, officials or agents of the Town who use, direct, or control a social media account.

2.3 General Provisions

While Users may use any form of social media for personal use while off-duty, their status as employees or agents of the Town requires that the content of any social media postings not be in violation of existing Town by-laws, policies, directives, rules or regulations.

The same basic principles and guidelines found in the Town's policies apply to employee activities online. Ultimately, Users are solely responsible for the information or images they communicate and/or post online. Before creating an online account or profile, Users should consider some of the risks and rewards that are involved. Users should keep in mind that any conduct that adversely affects job performance, the performance of other Town employees or otherwise adversely affects co-workers, residents, officials, suppliers, people who work on behalf of the Town or the Town's legitimate business interests may result in disciplinary action up to and including termination. While Town employees have the First Amendment right to free speech, that right is not absolute and extends only to matters of public concern.

2.4 Using Social Media At Work

The Town of NAME permits employees to use the Internet for limited personal use. Refrain from using social media while on work time or on equipment provided by the Town, unless it is work-related as authorized by your manager or consistent with the Technology Use Policy. Access to and use of social media must not interfere with employees' productivity and/or ability to perform their duties and responsibilities.

2.5 Know And Follow The Rules

Carefully read this Policy and review the Town's Code of Conduct, Non-Discrimination Policy and the Town's Discrimination and Harassments Prevention Policy and ensure your postings are consistent with these policies. Inappropriate postings that include discriminatory remarks, harassment, and/or threats of violence or similar inappropriate or unlawful conduct will not be tolerated and may subject you to disciplinary action up to and including termination. All Users shall comply with the following:

- Online postings that harass or threaten other Town employees or officials are expressly prohibited. Harassing or discriminatory posts or comments may be deemed inappropriate in violation of this Policy, even if the Town or the names of any of its employees are not posted or "tagged" in the comment.

- Online postings that disparage others based on race, national origin, sex, sexual orientation, age, disability or religion are not permitted under any circumstances, regardless of the time, place, form or manner in which the information is posted or transmitted.

- Maintain the privacy of confidential information. Do not post internal reports, policies, procedures or other internal confidential communications. Users are prohibited from posting nonpublic items that are gained as a result of their position with the Town.

- Users may not use social media to engage in any activity or conduct that violates federal, state, or local law. Examples include, but are not limited to, software piracy or child pornography.

2.6 Be Respectful

Always be respectful of fellow co-workers, residents, suppliers and vendors. Also, remember that you are more likely to resolve work-related disputes by speaking directly with your co-workers than by posting complaints to a social media outlet. Nevertheless, if you decide to post complaints or criticism, avoid using statements, photographs, video or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating, that might constitute harassment or bullying, or that disparages fellow co-workers, residents, suppliers or vendors.

2.7 Be Honest And Accurate

Always post honest and accurate information or news, and if you make a mistake, correct it quickly. Be honest about any previous posts you have altered or edited. Remember that the Internet archives almost everything; therefore even deleted postings can be searched. Never post any information or rumors you know to be false about the Town, Town officials, fellow co-workers, citizens, suppliers or vendors.

2.8 Do Not Post On Behalf Of The Town Without Prior Authorization

Do not use your Town email address to register on social networks, blogs or other online tools utilized for personal use.

Do not create a link from your social networking site, blog, or other website to a Town website without identifying yourself as a Town employee.

Express only your personal opinions. Never represent yourself as a spokesperson for the Town. If you are writing about the Town, make it clear that you are not speaking on behalf of the Town. Specifically express that while you are an employee of the Town, your views do not represent those of the Town, fellow co-workers, citizens, suppliers, vendors, or anyone working on behalf of the Town. Include a disclaimer, such as "The postings on this site express my own views, positions and opinions, and do not necessarily reflect the views of the Town of [INSERT NAME]."

Employees should not speak to the media on the Town's behalf without contacting [INSERT MEDIA CONTACT PERSON]. Employees should not post a message that is in the Town's name or may be attributed to the Town without first obtaining prior authorization.

3.0 Expectation Of Privacy

Any information stored, accessed, browsed and/or created using the Town's technology, including its network/systems should not be considered private by the user. This includes, but is not limited to, any and all electronically stored information and electronic files, electronic mail communications, Internet website history, text messages, telephone call history, and voice mail. Even though employees are issued a password or other private access code, they should have no expectation of privacy with regard to the use of the Town's computers and/or network. All aspects of the Town's network/system usage by a user is subject to monitoring, the Massachusetts Records Law, and legal discovery, as applicable.

Users of social media are cautioned that they should have no expectation of privacy while using the Internet. Online postings can be reviewed by anyone, including the Town. Employees should presume that all social media postings, regardless of privacy settings, are public and use their best judgment when participating in social media.

4.0 Enforcement

4.1 Violations

Failure to comply with the Town of NAME's Acceptable Use Policy may result in either the suspension or permanent loss of the privilege to use the Town's technology resources. Users shall report violations of this Policy to their supervisor or, in the case of department heads, directly to the Town Administrator and/or Human Resources. Such violations include electronic and online conduct that adversely affects the employee's job performance, the performance of fellow employees or otherwise adversely affects the citizens, suppliers, vendors, people who perform work on behalf of the Town, or the Town's legitimate interest in serving the citizens of the Town of [INSERT NAME].

Violations of this Policy will be subject to disciplinary action, up to and including discharge. Additionally, users shall be personally liable for any losses, costs or damages incurred by the Town related to violations of this Policy.

4.2 Retaliation Is Prohibited

The Town prohibits taking adverse action against any employee for reporting a possible violation of this Policy or for cooperating in an investigation. Any employee who retaliates against another for reporting a possible violation of this Policy or for cooperating in an investigation will be subject to disciplinary action, up to and including discharge.

5.0 Acknowledgement

Town employees and users must sign a written acknowledgement that they have received, read, understand, and agree to comply with the Town of NAME's Acceptable Use Policy.

[INSERT TOWN NAME]
Acceptable Use Policy

ACKNOWLEDGEMENT FORM

I have received a copy of the Town of [INSERT NAME]'s Acceptable Use Policy.

I understand that this policy replaces any and all prior verbal and written communications regarding Town policies relating to the use and access of the Town's technology resources and social media, and Town monitoring of these activities as defined in the Policy.

I have read and understand the contents of the Acceptable Use Policy and agree to abide by its terms.

I understand that if I have questions or concerns at any time about the Acceptable Use Policy, I will consult my immediate supervisor, my supervisor's manager, the Human Resources Department, or the Technology Department for clarification.

I understand that the contents of the Acceptable Use Policy may change at any time.

Declaration

I have read, understand and acknowledge receipt of the Town of NAME Acceptable Use Policy. I will comply with the guidelines set forth in this Policy and understand that failure to do so may result in disciplinary or legal action.

_____ _____

SIGNATURE DATE

_____

PRINTED NAME

6. Body Worn Camera Policy

Purpose:

This policy is intended to provide officers with instructions on when and how to use body-worn cameras so that officers may reliably audio and video record their contacts with the public in accordance with applicable Massachusetts laws.

Policy:

It is the policy of the Employer Police Department that officers shall activate the body worn camera when such use is appropriate to the proper performance of his or her official duties, consistent with Massachusetts law and Federal law. This policy does not govern the use of surreptitious recording devices used in undercover operations.

The use of the portable video recording system provides persuasive documentary evidence for criminal investigations, internal or administrative investigations, and civil litigation. Officers shall utilize this device in accordance with the provisions in this general order to maximize the effectiveness of the audio/video documentation to achieve operational objectives and to ensure evidence integrity.

Procedures:

1. Objectives Of The Body Worn Camera Program

A. The Employer Police department has adopted the use of body worn cameras to accomplish several objectives. The primary objectives are as follows:

1. Body worn cameras allow for accurate documentation of police-public contacts, arrests, and critical incidents. They also serve to enhance the accuracy of officer reports and testimony in court.

2. Audio and video recordings also enhance this agency's ability to review probable cause for arrest, officer and suspect interaction, and evidence for investigative and prosecutorial purposes and to provide additional information for training purposes.

3. The body worn camera may also be useful in documenting crime and accident scenes or other events that include the confiscation and documentation of evidence or contraband.

2. When And How To Use The Body Worn Camera

A. Officers shall activate the body worn camera to record all contacts with citizens in the performance of official duties. It shall be the responsibility of each individual officer to test the body worn camera equipment at the beginning of each tour of duty. Officers equipped with the body worn camera will ensure that the batteries are charged prior to the beginning of their shift or special event. In the event that the equipment is found to be functioning improperly, the officer shall report the problem immediately to their immediate supervisor so that the information can be documented, and arrangements made for repair.

B. Whenever possible, officers should inform individuals that they are being recorded. In locations where individuals have a reasonable expectation of privacy, such as a residence, they may decline to be recorded unless the recording is being made pursuant to an arrest or search of the residence or the individuals. The body worn camera shall remain activated until the event is completed in order to ensure the integrity of the recording, unless the contact moves into an area restricted by this policy.

C. If an officer fails to activate the body worn camera, fails to record the entire contact, or interrupts the recording, the officer shall document why a recording was not made, was interrupted, or was terminated.

D. Uniformed officers assigned body worn cameras will wear them at all times while on duty in any type of uniform. Body worn cameras will be worn according to manufacturer's specifications and/or recommendations. Officers will make every reasonable effort to ensure that the body worn camera recording equipment is capturing events by positioning and adjusting the body worn camera to record the event.

E. Police personnel shall use only body worn cameras issued by the Employer Police Department. The body worn camera equipment and all data, images, video, and metadata captured, recorded, or otherwise produced by the equipment is the sole property of the Employer Police Department.

F. Police personnel who are assigned body worn cameras must complete an agency approved and/or provided training program to ensure proper use and operations prior to wearing the camera. Additional training may be required at periodic intervals to ensure the continued effective use and operation of the equipment, proper calibration

and performance, and to incorporate changes, updates, or other revisions in policy and equipment.

G. Officers are encouraged to inform their supervisor of any recordings that may be of value for training purposes.

H. Officers shall note in the incident report, the arrest report, or related reports when recordings were made. However, body worn camera recordings are not a replacement for written reports.

3. Restrictions On The Use Of Body Worn Cameras

A. Body worn cameras shall be used only in conjunction with official law enforcement activities. The body worn camera shall not be used to record:

1. Communications with other police personnel without the permission of the chief of police or his/her designee.

2. When on break or otherwise engaged in personal activities.

3. Encounters with undercover officers or confidential informants.

4. In any location where individuals have a reasonable expectation of privacy, such as a restroom or locker room.

4. Storage

A. All files shall be securely downloaded periodically and no later than the end of each shift. Each file shall contain information related to the date, body worn camera identifier, and assigned officer.

B. All images and sounds recorded by the body worn camera are the exclusive property of the Employer Police Department. Accessing, copying, or releasing files for non-law enforcement purposes is strictly prohibited.

C. All access to body worn camera data (images, sounds, and metadata) must be specifically authorized by the Chief of Police or his/her designee, and all access is to be audited to ensure that only authorized users are accessing the data for legitimate and authorized purposes.

D. Files should be securely stored in accordance with state records retention laws and no longer than useful for purposes of training or for use in an investigation or prosecution.

5. Supervisory Responsibilities

A. Supervisory personnel shall ensure that officers equipped with body worn camera devices utilize them in accordance with policy and procedures defined herein.

B. At least on a monthly basis, supervisors will randomly review body worn camera recordings to ensure that the equipment is operating properly and that officers are using the devices appropriately and in accordance with policy and to identify any areas in which additional training or guidance is required.