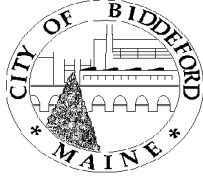


City of Biddeford
Personnel Committee
August 18, 2020 3:00 PM Zoom

- 1. Call to Order**
- 2. Acceptance of Minutes**
 - 2.1. Minutes
[Minutes 7-21-20.docx](#)
- 3. Discussion**
 - 3.1. Safety Committee Update
[Safety Brief 8-18-20.docx](#)
 - 3.2. Performance Reviews Updates
[Perf Review Brief.docx](#)
 - 3.3. E-media Language Discussion
[E-media Policy edits 8-18.docx](#)
- 4. Other Business**
- 5. Adjourn**



PERSONNEL COMMITTEE MEETING

Tuesday July 22, 2020
Human Resources Department

3 PM

Minutes

ITEM 1 Call to order

Chair Councilor Michael Ready called the meeting to order at 3 PM with Councilors William Emhiser, and Robert Quattrone Jr. present. Also present were James Bennett, City Manager, Diana DePaolo, Human Resources Director, and Hillary Owens, Management Analysis

ITEM 2 Acceptance of Minutes

Minutes from June 16, 2020 meeting accepted

ITEM 3

Item 3.1 Electronic Media Policy

Decisions for change in policy tabled until later date so that Norm Belanger can be in attendance.

ITEM 4 Other Business

Continued discussion in regard to alternative work arrangements. Jim Bennett to research online self-service activity vs. in office. Committee to discuss what their recommendation is.

ITEM 5 Adjourn



Personnel Committee

Meeting Date: Tuesday, August 18, 2020
Meeting Time: 3pm
Agenda Item No: 1
Item Description: Safety Update
Submitted by: Diana DePaolo, HR Director

Supporting Information/Documentation:

Information regarding new City processes, contacts, forms and MMA new risk management program attached

Key Terms:

Executive Summary:

Work is being done on a city wide and departmental basis to follow MMA's Risk Management Incentive Program.

Detailed Review:

A City Wide Safety Committee meeting was recently held with the liaison from each City Department and HR. Information was requested for Tier 1 of the Incentive Program. Each department is responsible for getting this information to HR prior to September 1st. Discussions focused on using the protocols departments currently have in place and simply documenting for the Program. Most departments stated that they are already doing most of what is needed to meet the Tier 1 requirement.

Funding Source:

n/a

Staff Recommendation:

*just providing update to committee



Personnel Committee

Meeting Date: Tuesday, August 18, 2020
Meeting Time: 3pm
Agenda Item No: 2
Item Description: Performance Review Update
Submitted by: Diana DePaolo, HR Director

Supporting Information/Documentation:

Key Terms:

Executive Summary:

.

Detailed Review:

The new Performance Review process is underway. 360 Review forms have gone out to all staff that directly report to a Department Head. Diana has begun meeting with Department Heads to go over the reviews for their staff. This is being done to give HR a general sense of performance level within each department and also to allow for feedback and review of new process so anything that may need to be adjusted or looked at again becomes apparent. On July 28th a training was held for the Department Heads on best practices regarding Performance Reviews and more specifically the actual meeting that takes place between employee and supervisor. The process seems to be going very well, many DHs told me they found the training to be informative and helpful and staff are happy with the forms.

Funding Source:

n/a

Staff Recommendation:

*just providing update to committee

ELECTRONIC MEDIA POLICY

A. Applicability: This policy applies to all full-time, part-time, contracted or seasonal employees, elected officials, volunteers, and other individuals who are provided access to the City's computer and electronic information systems. Third parties, as defined in Section 3, Definitions, should only be provided access to the system as necessary for their business purpose with the City and only if they abide by all applicable rules.

B. Purpose: The purpose of this policy is to provide guidance on appropriate use of electronic media services to include but not be limited to e-mail, Internet, VoIP, blogs, social media sites, or other means of access to resources made available to City of Biddeford employees to communicate with each other, other governmental entities and companies and individuals for the benefit of the City of Biddeford.

C. Definitions:

1. **Chat / Video Chat Service** means an informal online discussion in a chat room; a real-time online interactive discussion group.
2. **City's System** means the software, hardware and any other computer related equipment and/or programs that are obtained and licensed through the City of Biddeford
3. **Electronic Media Account** means any information or data accessed utilizing the City's System, including, but not limited to, Email, Social Media postings, Intranet communications, and Internet browsing history.
4. **E-mail** means a means or system for transmitting messages electronically; messages sent and received electronically through an email system.
5. **Executable File** means a file in a format that the computer can directly execute. Unlike source files, executable files cannot be read by humans.
6. **Incidental Use** means occasional or infrequent personal communication using City-owned computers and programs.
7. **Intranet** means a network operating like the World Wide Web but having access restricted to a limited group of authorized users (as employees of a company).
8. **Internet** means an electronic communications network that connects computer networks and organizational computer facilities around the world.
9. **Public Domain** means openly available to everyone. Non-copyrighted intellectual property that can be copied and freely distributed (but not sold) by anyone without a payment or permission.
10. **Social Media** means primarily Internet and mobile-based tools for sharing and discussing information. The term most often refers to activities that integrate technology, telecommunications and social interaction, alongside the construction of words, pictures, video and audio
11. **Social Media Site** means a website that leverages social media and communications tools for its visitors. Examples of social media sites include: YouTube, Flickr, Wikipedia, Twitter, Facebook, forum, message boards, etc.

12. **Third party** means individuals or groups who would not normally have access to the City's computer and information system but may from time to time require access to the systems. These could include, but are not limited to: hardware and software vendors, telephone system installers and contracted system troubleshooters, and auditors.

13. **Vandalism** is defined as any malicious attempt to harm or destroy data. This includes, but is not limited to, creating and/or knowingly uploading computer viruses.

D. Policy: The City's Systems are designed solely to facilitate City business communications among employees, residents and other business associates. Since no computer system is completely secure, care should be taken when transferring or discussing sensitive materials or subject matter.

These systems are the City of Biddeford's property and intended for City business. Although some incidental use of electronic services for personal use is expected, it must be understood that such use is a privilege, which may be limited or removed if the privilege is abused at any time, for any reason. All data and electronic messages within the City's Systems are the property of the City of Biddeford. **As such, no communications of any type can be considered private except as required by law.** Electronic communications have been found to be public records and may be subject to the freedom of access laws, depending on their content.

In addition, consistent with any confidential relationships or obligations with residents, employees, and Third-parties that may exist; the City of Biddeford reserves the right to authorize its directors, managers, and/or supervisors to review the contents of employee's Electronic Media Accounts when necessary for business or performance purposes, subject to the policies established by the City in connection with the exercise of such reviews.

E. Guidelines:

1. General Prohibitions: The City's Systems may be used only for lawful purposes. The transmission, distribution, or storage of any information, data, or material in violation of any applicable law or regulation, or provision of this policy is prohibited. Without limitation of the foregoing, it is prohibited to create, transmit, distribute or store any information, data, or material that:

- a. Is libelous, defamatory, hateful, or constitutes an illegal threat or abuse, or contains ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on race, national origin, sex, age, disability, sexual orientation, gender identity, religious beliefs or any other basis protected by law.
- b. Is obscene or constitutes child pornography, contains sexually explicit images or messages, or may be construed by a reasonable person as offensive, abusive or threatening.
- c. Knowingly infringes any copyright, trademark, trade secret, or other intellectual property right.
- d. Solicits for commercial ventures, religious or political causes, outside organizations or other non-job-related solicitations.
- e. Is or encourages conduct that would constitute a criminal offense or give rise to a civil liability.

- f. Is indented for personal gain.
- g. Solicits fundraising for profit or non-profit except as outlined in section F4, below.

2. General Guidelines: Employees are expected to abide by the generally accepted rules of computing and network etiquette. These include (but are not limited to) the following:

- a. Be polite
- b. Use appropriate language. Do not swear, use vulgarities or any other inappropriate language.
- c. Do not reveal private addresses or phone numbers of others unless available in the public domain and for legitimate business purposes. Providing both internal and your own personal address or phone number is a personal choice but be aware that electronic media transmissions can be monitored by others.
- d. Do not use computers or networks in such a way that you would disrupt their use by others. This includes being aware that you can create significant network traffic and consume scarce computing resources by your use of the Internet.
- e. Use only services you have authorization to access.
- f. Always represent yourself as yourself and as a representative of the City of Biddeford.
- g. Use proper judgment when sending un-encrypted confidential or proprietary information over the Internet. If you are uncertain whether material is confidential or proprietary, consult your supervisor. If you need to utilize encryption, please contact the IT Department for directions.
- h. Employees may not intentionally intercept, eavesdrop, record, read, alter, or receive other persons' e-mail messages without proper authorization.

3. Security Responsibilities:

- a. If you identify a security problem, notify the IT Department immediately.
- b. Do not show or identify a security problem to others.
- c. Do not reveal your account password or allow another person to use your account.
- d. Do not use another individual's account.
- e. Any user identified as a security risk may be subject to disciplinary action.
- f. Employees may not provide or use alternative software to access the systems. Employees may be held responsible for any damages caused by unauthorized software or viruses they knowingly or purposefully introduce.

- g. Employees should be aware that, due to retention policies or archiving, deletion of correspondence or posts may not result in deletion of the record from the City's centralized systems or servers controlled by other entities.
- h. Employees who leave employment with the City have no right to files, electronic communications, or access to City-related programs or sites except for each employee's personal employment records as may be managed by the HR Department or as may otherwise be required by law.
- i. All computer related equipment must be brought to the IT department for service, repair, or disposal. City owned computer equipment must be maintained under the direction of the IT Department.
- j. All City Computer related equipment must be purchased through or in coordination with the Computer Department
- k. Users may not store personal or non-work related material on the City's System.

4. Vandalism/Harassment/Legal Issues:

- a. Vandalism and/or harassment will result in disciplinary action.
- b. The misuse of Electronic Media Services may be considered sufficient cause for disciplinary action in accordance with the Personnel Policies and Procedures Manual, and/or other applicable rules or laws.
- c. In the event of suspected, alleged or actual illegal activity, the City of Biddeford may notify or cooperate with applicable law enforcement authorities for potential civil or criminal investigation or prosecution.

F. Media Specific Policies The City's System is intended to facilitate City business communication among employees, residents and other business associates for messages and memoranda. The following are considered acceptable uses for Email, the Intranet and the Internet:

1. Exchanging information directly related to work tasks
2. Education facilitating performance of any task or project related to assigned duties
3. Exchanging information for professional development, inquiry purposes, and research access for advisories, obtaining standards, finding statistics and analysis
4. The City understands that fellow employees would like to support the fundraising efforts of coworkers. To allow for this, the City has set up an email address: fundraising@biddefordmaine.org. You may subscribe to this email through the IT department if you would like to send or receive fundraising emails that coworkers are involved in.

G. Specific Prohibitions: Altering electronic communications to hide one's identity or to impersonate another individual is considered misrepresentation and is prohibited under this policy. All e-mail, news posts, chat sessions, or any other form of electronic communication must contain the sender's real name and/or e-mail address.

1. Initiating or forwarding "chain letters" or e-mail is prohibited on City's Systems and the Internet as a whole. Chain e-mail can be identified by phrases such as "please pass this on to your friends" or similar inducements that encourage the recipient to forward the message.
2. The practice of bombarding someone with a large volume of unsolicited mail in an attempt to disrupt them or their site is known as "mail bombing". Mail bombs have the effect of seriously degrading system performance and may have legal consequences. This practice is strictly prohibited on the City's Systems.
3. The practice of sending unsolicited commercial advertisements or solicitations (SPAM) via E-mail is regulated by applicable laws, and is prohibited.
 - City users found in violation of these laws could be subject to criminal prosecution, civil prosecution, administrative action, and/or loss of some or all computing privileges
4. Use of electronic communications, including E-mail, with the intent to annoy, harass and/or physically threaten other individuals is prohibited.
5. Use of City resources, including E-mail, for anyone's personal or political gain is prohibited. This includes promoting non-City sales and services.
6. Operation of unofficial E-mail reflectors is prohibited. An E-mail reflector is the automated or otherwise forwarding of a mail message to multiple recipients triggered by the content or headers of the mail message being forwarded.
7. E-mail messages may not include any user's identification number (e.g., social security number), should include only unique identifying information that is pertinent to the message being conveyed, and should not reference any confidential employee information.

H. Social Media: The City of Biddeford takes no position on your decision to start or maintain a blog or participate in other social networking activities. However, it is the right and duty of the City of Biddeford to protect itself from unauthorized disclosure of information.

1. **General Provisions:** Blogging or other forms of Social Media or technology include, but are not limited to video or wiki postings, sites such as Facebook and Twitter, chat rooms, personal blogs or other similar forms of online journals, diaries or personal newsletters not affiliated with the City of Biddeford.

Unless specifically instructed, employees are not authorized and therefore restricted to speak on behalf of the City of Biddeford. Employees may not publicly discuss vendors, projects, other employees or any work-related matters, whether confidential or not, outside company-authorized communications. Employees are expected to protect the privacy of the City of Biddeford and its employees and are prohibited from disclosing personal employee and nonemployee information and any other proprietary and nonpublic information to which employees have access. Such information includes but is not limited to customer information, employee information, protected citizen information, financial information and strategic business development.

City employees may not update, create or maintain personal blogs, Twitter, Facebook, and other Social Media site while on duty.

2. **Acknowledgement:** Employees are required to sign a written acknowledgement that they have received, read, understood and agreed to comply with the City's Electronic Media Policy.
3. **Personal Blogs and Social Media:** The City of Biddeford respects the right of employees to write blogs and use social networking sites as a medium of self expression and public conversation and does not want to discourage employees from self-publishing and self-expression. Employees are

expected to follow the guidelines and policies set forth to provide a clear line between you as the individual and you as the employee. The City of Biddeford does not discriminate against employees who use these media for personal interests and affiliations or other lawful purposes.

Bloggers and commenter's are personally responsible for their commentary on blogs and social networking sites. Bloggers and commenter's can be held personally liable for commentary that is considered defamatory, obscene, proprietary or libelous by any offended party, not just the City of Biddeford.

Employees cannot use blogs or social networking sites to harass, threaten, discriminate or disparage against employees or anyone associated with or doing business with the City of Biddeford. If you choose to identify yourself as a City of Biddeford employee, please understand that some readers may view you as a spokesperson for the City of Biddeford. Because of this possibility, we ask that you state your views expressed in your blog or social networking area are your own and not those of the City of Biddeford, nor of any person or organization affiliated or doing business with the City of Biddeford.

Employees cannot post on personal blogs or other sites the name or logo of the City of Biddeford or any business with a connection to the City of Biddeford. Employees cannot post City privileged information, including copyrighted information or City issued documents that are specifically protected and exempted from the Freedom of Information Act.

Employees cannot post on personal blogs or Social Media Sites photographs of other employees, clients, vendors, suppliers, or the general public taken while working for the City, nor can employees post photographs of persons engaged in City business or at City of Biddeford sanctioned functions.

Employees cannot post on personal blogs and social networking sites any advertisements or photographs associated with the City of Biddeford involving its logo, nor sell products and services under the City of Biddeford name or website.

Employees cannot link from a personal blog or social networking site to the City of Biddeford's internal or external web site.

If contacted by the media or press about their post that relates to the City of Biddeford business, employees are required to speak with their manager before responding.

If you have any questions relating to this policy, your personal blog or social networking, ask your manager or supervisor.

4. **Employer Monitoring:** Employees of the City of Biddeford are cautioned that they should have no expectation of privacy while using the Internet. Your postings can be reviewed by anyone, including the City of Biddeford. The City of Biddeford reserves the right to monitor comments or discussions about the City, its employees, clients and vendors, posted on the Internet by anyone, including employees and non-employees. The City of Biddeford has the capability of using blog-search tools and software to monitor forums such as blogs and other types of personal journals, diaries, personal and business discussion forums, and social networking sites.

Employees are cautioned that they should have no expectation of privacy while using the City's System or facilities for any purpose. However, investigations that include this type of monitoring

will only be performed under the direction of the City Manager or Chief Operating Officer and will not be done randomly or by any other staff person.

The City of Biddeford reserves the right to use content management tools to monitor and block content.

5. **Reporting Violations:** The City of Biddeford requests and strongly urges employees to report any violations or possible or perceived violations to supervisors, managers or the HR Department. Violations include discussions of the City of Biddeford and its employees, any discussion of proprietary information and any unlawful activity related to blogging or social networking that violates any Federal privacy law or discloses protected information under State and Federal law of either City of Biddeford employees or the public they serve.

I. Chat/Video Chat Services: Chat services are limited to those provided by the City, tech support programs or webinars. No other chat programs are allowed without a manager's approval.

J. Executable Files: Downloading of executable files from the Internet requires prior approval by the employee's Department Head and security evaluation by the Computer Department

K. Website Development & Domain Policies:

Usage and Limitations: Every attempt should be made to post documents in PDF format

1. All pages that represent the City will be hosted on the Biddefordmaine.org site.
2. Pages must be maintained to keep information relevant, accurate and up to date.
3. Incomplete pages must not be used. No "under construction"
4. Photo release forms must be on file in the IT Directors office for all non-employee photos.
5. All domain names must be purchased by the IT department and registered with the City's registrar under the City account.

Specific Prohibitions:

1. No links, posts or transmissions of any unlawful, threatening, libelous, harassing, defamatory, vulgar, obscene, pornographic, profane, or otherwise objectionable content.
2. All forms of advertising are prohibited

L. Enforcement:

1. **Disciplinary Action:** The City of Biddeford investigates and responds to *all* reports of violations of this policy and other related policies. Violation of the City's social networking policy will result in disciplinary action in accordance with the employee's union contract or personnel policy up to and including immediate termination. Discipline or termination will be determined based on the nature of the infraction. The City of Biddeford reserves the right to take legal action where necessary against employees who engage in prohibited or unlawful conduct.

2. **Grievance Procedure:** Any grievance as it relates to this policy should be brought to an immediate supervisor and or the HR department.

CELL PHONE POLICY

City-Issued Cell Phones: The City may issue cell phones to employees whose jobs require them to make calls while away from work or require them to be accessible for work-related matters. Cell phones issued by the City are City property. Employees who leave the City for any reason must turn in their City-issued cell phones.

City-issued cell phones are to be used primarily for business purposes. Although occasional, brief personal phone calls using a City-issued phone are permitted, employees are expected to reimburse the City for any additional costs or charges relating to texting or personal use of their cell phones.

Employees are responsible for the security of City-issued cell phones and the information stored on them. If your City-issued cell phone is lost or stolen, notify the City's IT Director and your Department Head immediately.

We are concerned for your safety and for the safety of other drivers and pedestrians, and using a cell phone while driving can lead to accidents. Employees are prohibited from using cell phones for work-related matters while driving, with the exception of recognized public safety emergencies.

If you must make a work-related call while driving, you must wait until you can pull over safely and stop the car before placing your call. If you receive a work-related call while driving, you must ask the caller to wait while you pull over safely and stop the car. If you are unable to pull over safely, you must tell the caller that you will have to call back when it is safe to do so.

Employees may use hands-free equipment to make or answer calls while driving without violating this policy. However, safety must always be your first priority. We expect you to keep these calls brief. If, because of weather, traffic conditions, or any other reason, you are unable to concentrate fully on the road, you must either end the conversation or pull over and safely park your vehicle before resuming your call.

Personal Cell Phones: Although we allow employees to bring their personal cell phones to work, we expect employees to keep personal conversations or text messaging to a minimum. While occasional, brief personal phone calls are acceptable, frequent or lengthy personal calls can affect productivity and disturb others. For this reason, we generally expect employees to make and receive personal phone calls and text messages during breaks only.

Employees must turn off the ringers on their cell phones while away from their cell phones. If you share workspace with others, please turn off the ringer on your phone while at work. Remember, others can hear your cell phone conversations. Try to talk quietly, and save intimate discussions for another time.

Employees should turn off their cell phones or leave their phones elsewhere while in meetings, presentations, or trainings. Employees must also turn off their cell phones or leave their phones elsewhere while meeting with clients or serving customers. It is inappropriate to interrupt a face-to-face conversation with a customer in order to take a personal phone call.

Employees who violate this policy will be subject to discipline, up to and including termination.

MOBILE DEVICE SECURITY

1. Introduction

Mobile devices, such as smart phones and tablet computers, are important tools for the organization and their use is supported to achieve business goals.

However, mobile devices also represent a significant risk to information security and data security if the appropriate security applications and procedures are not applied. They can be a conduit for unauthorized access to the organization's data and IT infrastructure. This can subsequently lead to data leakage and system infection.

The City of Biddeford has a requirement to protect its information assets in order to safeguard its customers, intellectual property and reputation. This document outlines a set of practices and requirements for the safe use of mobile devices.

2. Scope

1. All mobile devices, whether owned by the City of Biddeford or owned by employees, that have access to corporate networks, data and systems, not including city IT-managed laptops. This includes smart phones and tablet computers.
2. Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk assessment must be conducted and authorized by security management.

3. Policy

Technical Requirements

1. Devices must use stock operating systems.
2. Devices must be configured with a secure password that complies with Biddeford's password policy. This password must not be the same as any other credentials used within the organization.
3. With the exception of those devices managed by IT, devices are not allowed to be connected directly to the internal corporate network.

User Requirements

1. Users must report all lost or stolen devices to the City of Biddeford IT department immediately.
2. If a user suspects that unauthorized access to City data has taken place via a mobile device the user must report the incident to the IT department immediately
3. Devices must not be "jailbroken", "rooted" or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
4. Users must not load pirated software or illegal content onto their devices.
5. Applications must only be installed from official platform-owner approved sources. Installation of code from un-trusted sources is forbidden. If you are unsure if an application is from an approved source contact the City of Biddeford's IT department.
6. Devices must be kept up to date with manufacturer or network provided patches. At a minimum patches should be checked for weekly and applied at least once a month.
7. Devices must not be connected to a PC which does not have up-to-date and enabled anti-malware protection and which does not comply with corporate policy.

8. Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that City data is only sent through the city email system. If a user suspects that city data has been sent from a personal email account, either in body text or as an attachment, they must notify the City of Biddeford IT department immediately.
9. Any device that connects to the city network, email system or VPN must have been added to the Mobile Device Management (MDM) system by the City's IT department. Removal of the MDM software will result in immediate denied access to city system(s)

*To jailbreak a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software.

4. Right to Privacy

Adding your phone to the City MDM will allow the city the following rights.

1. Wipe phone - This is used in the event the phone is lost or stolen
2. Enforce the use of a passcode
3. Clear passcode- This is used in the event a user forgets his or her passcode
4. Lock device
5. View device location (only if GPS is enabled) - This is used to locate lost or stolen devices
6. Push notifications - This could be used later for employee specific alerts
7. Application list - A list of installed applications will be sent to the MDM

In an effort to alleviate concerns, let it be known that the MDM has no way to see camera views, listen to audio or phone calls.