

CITY OF MEDFORD CELL PHONE/ WIRELESS DEVICE POLICY

SECTION I. PURPOSE

It is the policy of the City of Medford to provide cellular telephones to designated employees in order to improve productivity, enhance customer service to our citizens, and/or to enhance public safety services.

It is also the policy of the City to maintain the right of access and disclose any and all messages communicated through electronic means when City-owned equipment is used. Regardless of the intent of the message (business or personal), any employee involved has no right to privacy, or to the expectation of privacy, concerning the content of any message or the intended destination of any message.

Decisions regarding the use of City cellular telephones, which are not explicitly stated herein will be left to the discretion of the City Administrator. Department Heads are authorized to administer, provide guidance on, and assure compliance with the features of this policy.

SECTION II. PROCEDURE

1. Applicability

This Policy and Procedure applies to all City employees, departments, and organizations. This policy includes City-owned cellular telephones, electronic paging devices, and other wireless personal communications devices, which are not directly connected to a telephone line. It does not apply to direct wired landline telephones.

2. Authorized Usage

City-owned cellular telephones, electronic paging devices, and other wireless personal communications devices are primarily intended for City business. Minimal personal use of City-owned cell phones is allowed as long as the City does not accrue charges for minutes used in excess of the City's cell phone plan, and any other fee—roaming, long distance, etc—that is not part of the City's cell phone plan. Any additional fee on the City's account statement will be investigated and the employee responsible for accruing said fee shall reimburse the City for the charges.

Employee shall not use cellular telephones to discuss confidential or sensitive City business; cellular telephone conversations are not secure.

3. Eligibility Criteria

Employees eligible for assignment of City-owned cellular telephones, electronic paging devices, and other wireless personal communication devices are those designated by the City Administrator, including (but not limited to):

- a. Employees who are frequently in a vehicle, if the individual must conduct City business by telephone while in the field, and it can be shown that cost savings and customer service efficiency will be realized through use of such devices;
- b. Employees who have critical need to maintain accessibility with other department heads, city management staff and public officials, in order to insure uninterrupted customer services and/or the integrity of the organizations;
- c. Employees who have a responsibility for responding to public safety and emergency incidents in the field.

4. Responsibilities of Department Heads

The Department Heads are responsible for:

- a. Recommending requests for cellular telephones, electronic paging devices, and other wireless personal communications devices from their respective subordinates;
- b. Insuring that requests are in conformance with the procedures outlined herein, or that exceptions are justified;
- c. Insuring that all persons assigned a City-owned cellular telephone, electronic paging device, and/or other wireless personal communications device, are provided access to a copy of this policy, and that the individual is in compliance with it;
- d. Conducting annual reviews of assigned devices to determine if such assignments continue to be justified; and
- e. Informing appropriate employees responsible for City communications of all reassignments of cellular telephones, electronic paging devices, and other wireless personal communications devices.

5. Responsibilities of Employees

Employees who are assigned the use of City-owned cellular telephones, electronic paging devices, and other wireless personal communications devices are responsible for the following:

- a. Insuring the physical security of such devices;
- b. Insuring that all communications on such devices are kept to the briefest duration possible;
- c. Keeping personal communications to a minimum;
- d. Insuring that any personal use does not detract from the employee's availability for completion of assigned duties; and
- e. Reimbursing the city for any personal calls/fees sent or received at the rate established by the City Administrator.

6. Use of Electronic Communications Devices and Safe Driving

- a. All City employees are expected to drive with safety as the first consideration. Cell phone use, including text messaging, shall not be used in any manner which violates State Law. Employees are responsible for, and will be held accountable for, safe driving at all times.

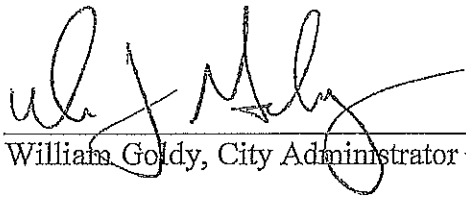
7. General Statements on Use of Wireless Communications Devices

- a. Use of a log-on or password does not imply any right to employee privacy of communication.
- b. On City-owned wireless communications devices, the City or department reserves the right to monitor and record communications traffic at any time, without notice to any employee.
- c. Any abuse or inordinate use of those devices will be considered misconduct and indifference to work, resulting in possible disciplinary action, up to and including termination. Any employee responsible for inordinate use of wireless communications devices may also be held responsible for the resulting costs to the City.

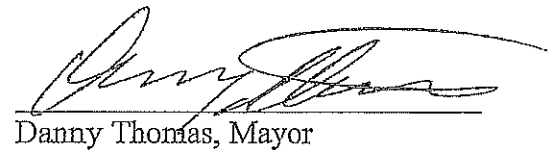
SECTION III. Approval of Policy

This policy shall be formally approved and adopted by the Medford City Council.

Adopted by the Medford City Council this 21st day of December, 2009.



William Goldy, City Administrator



Danny Thomas, Mayor

Medford Pool:

Lifeguard Manual

SUMMER 2026



Table of contents:

Job Description-----	page 3
Employment Policies-----	page 3-5
Performance Standards-----	page 5
Opening and Closing Procedures-----	page 6
Pool Rules-----	page 7
Lifeguard Employee Contract-----	page 8
Sub Request Form-----	page 9
Emergency Action Plans-----	page 10-11

Medford Pool:

Job Title: Lifeguard

Supervisor: Morgan Langeslag

Purpose:

Provide supervision, maintain accurate count of pool users, distribute concession items, enforce policies, and administer life saving techniques when necessary to all patrons using the pool.

Specific Duties and Responsibilities:

- Enforce all aquatic facility policies, rules, and regulations
- Recognize and respond effectively to emergency situations
- Inspect the aquatic facilities and report unsafe conditions and equipment to the manager
- Actively guard and scan the pool area at all times; refrain from socializing while guarding
- Secure the pool area by clearing the pool area when a lifeguard is not on duty
- Attend and participate in mandatory trainings and in-service trainings

Lifeguard Employment Policies:

Scheduling – Work schedules are completed before the season. Before the beginning of the season, you will be asked to fill out an Availability Form. The managers will develop a schedule based on all lifeguard's availability and will confirm the schedule with all guards before it is finalized.

Paychecks – Paychecks are distributed every other Friday.

Certification Reimbursement - A lifeguard who has obtained an initial lifeguard certification is eligible for reimbursement of up to half of the cost of the initial certification. The guard must work an entire pool season to receive reimbursement. A copy of the invoice for the course must be submitted to the City within a month of the end of the pool season.

A lifeguard who has obtained an initial WSI certification is eligible for reimbursement of up to half of the cost of the initial certification. The guard must work an entire pool season as a WSI to receive the reimbursement. A copy of the invoice for the course must be submitted to the City within a month of the end of the pool season.

Submitting Hours – All lifeguards are responsible for recording their **own** hours by punching in and out using the punch clock. Lifeguards must sign time cards by the final workday of the pay period. If you forget to punch in, have a manager write in the time **and** sign it. Pay period is Monday-Sunday.

Substitutions – Lifeguards are responsible for covering hours that they are scheduled to work. In the event you are not able to work, it is your responsibility to find a substitute lifeguard. This is done by filling out the 'request a sub' form found in the shack. It is also suggested that you call/email all other guards to try and find a sub. You are responsible for your shift until another guard has signed the form, and it is approved by management.

Phone/Email – Make sure the managers have the most up to date contact information for you in order to get in contact with you. Check your messages and voicemail often!

Tardiness – You are expected to be in uniform and ready to be in the stand five (5) minutes before you are scheduled.

Uniform - The lifeguard uniform worn by guards while teaching swimming lessons includes any one-piece swimming suit (women), swimming trunks (men), and your whistle. The lifeguard uniform worn by guards for all shifts other than teaching swimming lessons includes a one-piece or two-piece swimming suit (women), swimming trunks (men), and your whistle.

- All swimsuits (other than boardshorts) should be athletic-style. The swimsuit must be of a full-coverage style that provides adequate coverage of the chest and buttock. All other styles of swimwear are prohibited. (See prohibited styles below.)
 - Swimsuit bottoms and tops are not to have tie fasteners.
 - Swimsuit bottoms and tops are not to be tugged, rolled, pinned, or adjusted in any way to reduce coverage.

- **Prohibited swim bottom styles:** gstring, thong, Brazilian, cheeky, low-cut, suits that fasten with a tie at the side, bottoms with venting or cutouts.
- **Prohibited swim top styles:** string bikini, triangle top, tops with venting or cutouts, any style that has a tie fastener.

Example of Acceptable Uniform:



Breaks – Lifeguards will be given a 10-minute break in between the hour shifts on the stand. The rotation begins with low stand (1 hour), then high stand (1 hour), and ends with an hour in the shack. **UNDER NO CIRCUMSTANCES SHOULD THE POOL BE WITHOUT A LIFEGUARD ON THE POOL DECK!**

Secondary Guard – As the secondary guard who is not on the stand and in the shack, it is your responsibility to record patron counts, and support the primary guards as needed. During this time in the shack, you are expected to be assisting anyone that needs assistance. The PATRONS come before anything else! There are duties to be done at all times, and you must be in the position to react to an emergency as necessary.

Food Consumption – You may bring food and beverages to consume on your break. These may be stored in the refrigerator. If you take candy or anything from the shack, you **MUST** pay for it! Nothing is free for the lifeguards. Daily inventory is taken!

In-service Training – Your attendance at the prescheduled in-service trainings is **MANDATORY**. You will be paid for attending and participating. Dates and times of meetings will be posted in the shack, as well

as communicated to you well in advance. If you are unable to attend the scheduled in-services, you must schedule a make up with one of the managers immediately. It is your responsibility to keep the certifications current that are required for your position current.

Emergency Phones – There is a phone located in the shack. When opening the pool, check the phone to ensure that it is functioning. Patrons are not to use the office phone, unless granted permission.

Lost and Found – Lost and Found articles are kept in the shack.

Cleaning – Throughout each shift, lifeguards must perform cleaning duties as assigned.

Counts –Record how many people enter the pool during each shift. Record these counts in the binder by the front window. Make sure that people are paying the correct amount when they enter the pool.

\$20: Weekly Pass \$5: All Day \$3: Single Session (3 and under only- \$3 all day, \$1 single session)

Evaluations – All of the elements within this manual will all be taken into consideration at the end of the summer for individual evaluations performed by the managers.

Cell Phones - Absolutely no cell phones are allowed on the guard stand or around you while you are on duty. Please leave your cell phone with your personal belongings which should be stored in the shack. If you need to make a call, do so while on your break.

Lifeguard Performance Standards:

- The primary responsibility of a lifeguard is to protect the safety and well-being of each person using the pool. No other duty should jeopardize this primary responsibility.
- Never leave the pool unattended!
- Both lifeguards must be in the guard stands, once at least six patrons enter the pool.
- Promptly enforce all rules and regulations specifically showering and no shallow water diving. Stop all unsafe actions and report all unsafe conditions to the managers or City Administrator.
- Lifeguards must have a rescue tube, and rescue pack on the stand. A whistle must be worn at all times while on duty.
- Refrain from talking extensively with patrons or having visitors when on duty. Conversations with patrons should be kept brief and to a minimum.
- Remain alert at all times. This is demonstrated by good posture, proper positioning at your station, using a method of zone coverage and having a constant awareness of your surroundings.

Opening Procedures

1. Open the gates and bathroom doors, and remove the noodles, water aerobics items, and backboard from inside. Ensure that they are ready to use.
2. Remove the pool covers.
3. Retrieve the vacuum from the garbage can, and the pole from the chemical room, and vacuum the **ENTIRE** length of the pool. This can take a long time, depending on how dirty the pool is from the previous day.
4. Put on your PPE and check all of the drains. Clean them out, and be prepared for any surprises! Take the garbage bucket from the chemical room and empty the debris into there.
5. Take out the water aerobics sign-up sheet and money box (if it is a weekday).
6. Before pool opens, ensure no items/debris or garbage are inside or outside the pool. If items do exist, retrieve them and place in appropriate area.
7. Retrieve rescue tubes and hip packs from the shack and put at the lifeguard stands.
8. Observe all other areas of the pool to ensure no issues exist that would halt the pool opening.
9. Turn the radio on.
10. Put the rope into the pool before opening for patrons.
11. If you notice anything that you are uncomfortable with for an opening, contact the pool manager and/or the city administrator immediately.

Closing Procedures

1. The lifeguard in the shack during the last hour of the night, has the responsibility of cleaning the bathrooms. This includes: scrubbing, washing, and drying the floors, picking up garbage and toilet paper, taking out the garbage (including the one in the women's stall), and replacing the toilet paper or hand towels as needed.
2. Make rounds around the vicinity to make sure all candy wrappers and garbage is picked up.
3. Blow your whistle at the appropriate time, and make sure all patrons exit the pool before the lifeguard's head to the shack. Carefully watch the pool area until everyone leaves.
4. Remove the rope from the water and place back into the chemical room. Once all patrons have left the pool area, ensure all pool items are removed from the pool.
5. The assigned lifeguard will stay for water aerobics. This person must be out with the patrons in attendance, and not in the shack.
6. Make sure the shack is neat and clean before you leave for the day.
7. The last lifeguard to leave will turn off all lights, radios **AND** Wi-Fi.

POOL RULES:

1. Suit requirements: no cut-offs, fringes, cut-off sweatpants, or diapers are allowed.
2. No one is allowed into the pool area unless a lifeguard is present.
3. Patrons must shower before entering the water.
4. No food, pop, or candy is allowed near the pool.
5. No horseplay, splashing, dunking, etc. is allowed.
6. No back entries, back dives, or back flips are allowed.
7. No spitting, spouting water or blowing nose is allowed.
8. No toys, inflatables, masks, snorkels, etc. are allowed EXCEPT in Toy and Family nights.
9. The "Warning System" will be enforced to discipline patrons using unsafe, inappropriate or immature behavior.
10. All patrons must practice safe behavior at the pool facility.

THE LIFEGUARD ALWAYS HAS COMPLETE AUTHORITY OVER THE POOL AREA.

Whistle Communication:

One short blast: alert patron of rules (shower, please walk, no diving, etc.)

Two short blasts: going in for rescue; alert other lifeguard of coverage (getting off stand, need assistance, etc.)

Medford Pool- Summer 2026

Lifeguard Employee Contract

By signing this contract, I agree to:

- Support and abide by all policies, procedures and regulations as set forth by the Employee Handbook.
- Perform in good faith all duties and responsibilities described in the Lifeguard Manual, job description, personnel memorandums, and discussions at employee in-service training sessions, and meetings.
- Represent the Medford Pool in an honest, positive and professional manner at all times.



Print Name:

Signature Date:

Manager Signature:

Received Date:

City Administrator Signature:

MEDFORD POOL TIME OFF/SUBSTITUTE REQUEST FORM

DATE: _____

NAME: _____ PHONE NUMBER: _____

DATE(S) NEEDED OFF: _____ TIME(S) NEEDED OFF: _____

REASON: _____

SUB NAME: _____ SUB SIGNATURE: _____

SUPERVISOR INITIALS: _____ SUB PHONE: _____

IF MISSING ANY CLASSES, WHAT CLASS OR CLASSES?

CLASSES: _____ TIMES: _____

Employee's Withholding Certificate

OMB No. 1545-0074

Complete Form W-4 so that your employer can withhold the correct federal income tax from your pay.

Give Form W-4 to your employer.

Your withholding is subject to review by the IRS.

2026**Step 1:**
Enter
Personal
Information

(a) First name and middle initial	Last name	(b) Social security number
Address		Does your name match the name on your social security card? If not, to ensure you get credit for your earnings, contact SSA at 800-772-1213 or go to www.ssa.gov .
City or town, state, and ZIP code		
(c) ☐ Single or Married filing separately ☐ Married filing jointly or Qualifying surviving spouse ☐ Head of household (Check only if you're unmarried and pay more than half the costs of keeping up a home for yourself and a qualifying individual.)		
Caution: To claim certain credits or deductions on your tax return, you (and/or your spouse if married filing jointly) are required to have a social security number valid for employment. See page 2 for more information.		

TIP: Consider using the estimator at www.irs.gov/W4App to determine the most accurate withholding for the rest of the year if you: are completing this form after the beginning of the year; expect to work only part of the year; or have changes during the year in your marital status, number of jobs for you (and/or your spouse if married filing jointly), dependents, other income (not from jobs), deductions, or credits. Have your most recent pay stub(s) from this year available when using the estimator. At the beginning of next year, use the estimator again to recheck your withholding.

Complete Steps 2–4 ONLY if they apply to you; otherwise, skip to Step 5. See page 2 for more information on each step, who can claim exemption from withholding, and when to use the estimator at www.irs.gov/W4App.

Step 2:
Multiple Jobs
or Spouse
Works

Complete this step if you (1) hold more than one job at a time, or (2) are married filing jointly and your spouse also works. The correct amount of withholding depends on income earned from all of these jobs.

Do **only one** of the following.

- (a) Use the estimator at www.irs.gov/W4App for the most accurate withholding for this step (and Steps 3–4). If you or your spouse have self-employment income, use this option; or
- (b) Use the Multiple Jobs Worksheet on page 3 and enter the result in Step 4(c) below; or
- (c) If there are only two jobs total, you may check this box. Do the same on Form W-4 for the other job. This option is generally more accurate than Step 2(b) if pay at the lower paying job is more than half of the pay at the higher paying job. Otherwise, Step 2(b) is more accurate ☐

Complete Steps 3–4(b) on Form W-4 for only ONE of these jobs. Leave those steps blank for the other jobs. (Your withholding will be most accurate if you complete Steps 3–4(b) on the Form W-4 for the highest paying job.)

Step 3: Claim Dependent and Other Credits	If your total income will be \$200,000 or less (\$400,000 or less if married filing jointly):			
	(a) Multiply the number of qualifying children under age 17 by \$2,200	3(a)	\$	
	(b) Multiply the number of other dependents by \$500	3(b)	\$	
	Add the amounts from Steps 3(a) and 3(b), plus the amount for other credits. Enter the total here		3	\$
Step 4: Other Adjustments	(a) Other income (not from jobs). If you want tax withheld for other income you expect this year that won't have withholding, enter the amount of other income here. This may include interest, dividends, and retirement income		4(a)	\$
	(b) Deductions. Use the Deductions Worksheet on page 4 to determine the amount of deductions you may claim, which will reduce your withholding. (If you skip this line, your withholding will be based on the standard deduction.) Enter the result here		4(b)	\$
	(c) Extra withholding. Enter any additional tax you want withheld each pay period		4(c)	\$

Exempt from withholding	I claim exemption from withholding for 2026, and I certify that I meet both of the conditions for exemption for 2026. See <i>Exemption from withholding</i> on page 2. I understand I will need to submit a new Form W-4 for 2027 ☐		
Step 5: Sign Here	Under penalties of perjury, I declare that this certificate, to the best of my knowledge and belief, is true, correct, and complete.		
Employers Only	Employee's signature (This form is not valid unless you sign it.)		Date
	Employer's name and address	First date of employment	Employer identification number (EIN)



Employment Eligibility Verification

Department of Homeland Security
U.S. Citizenship and Immigration Services

USCIS
Form I-9

OMB No.1615-0047
Expires 05/31/2027

START HERE: Employers must ensure the form instructions are available to employees when completing this form. Employers are liable for failing to comply with the requirements for completing this form. See below and the Instructions.

ANTI-DISCRIMINATION NOTICE: All employees can choose which acceptable documentation to present for Form I-9. Employers cannot ask employees for documentation to verify information in Section 1, or specify which acceptable documentation employees must present for Section 2 or Supplement B, Reverification and Rehire. Treating employees differently based on their citizenship, immigration status, or national origin may be illegal.

Section 1. Employee Information and Attestation: Employees must complete and sign Section 1 of Form I-9 no later than the **first day of employment**, but not before accepting a job offer.

Last Name (Family Name)		First Name (Given Name)		Middle Initial (if any)	Other Last Names Used (if any)		
Address (Street Number and Name)			Apt. Number (if any)	City or Town		State	ZIP Code
Date of Birth (mm/dd/yyyy)	U.S. Social Security Number		Employee's Email Address			Employee's Telephone Number	
I am aware that federal law provides for imprisonment and/or fines for false statements, or the use of false documents, in connection with the completion of this form. I attest, under penalty of perjury, that this information, including my selection of the box attesting to my citizenship or immigration status, is true and correct.		Check one of the following boxes to attest to your citizenship or immigration status (See page 2 and 3 of the instructions.):					
		☐ 1. A citizen of the United States					
		☐ 2. A noncitizen national of the United States (See Instructions.)					
		☐ 3. A lawful permanent resident (Enter USCIS or A-Number.)					
		☐ 4. An alien authorized to work until (exp. date, if any)					
		If you check Item Number 4., enter one of these:					
		USCIS A-Number	OR	Form I-94 Admission Number	OR	Foreign Passport Number and Country of Issuance	
Signature of Employee					Today's Date (mm/dd/yyyy)		

If a preparer and/or translator assisted you in completing Section 1, that person **MUST** complete the Preparer and/or Translator Certification on Page 3.

Section 2. Employer Review and Verification: Employers or their authorized representative must complete and sign Section 2 within three business days after the employee's first day of employment, and must physically examine, or examine consistent with an alternative procedure authorized by the Secretary of DHS, documentation from List A OR a combination of documentation from List B and List C. Enter any additional documentation in the Additional Information box; see Instructions.

List A		OR	List B	AND	List C
Document Title 1					
Issuing Authority					
Document Number (if any)					
Expiration Date (if any)					
Document Title 2 (if any)		Additional Information			
Issuing Authority					
Document Number (if any)					
Expiration Date (if any)					
Document Title 3 (if any)					
Issuing Authority		☐ Check here if you used an alternative procedure authorized by DHS to examine documents.			
Document Number (if any)					
Expiration Date (if any)					

Certification: I attest, under penalty of perjury, that (1) I have examined the documentation presented by the above-named employee, (2) the above-listed documentation appears to be genuine and to relate to the employee named, and (3) to the best of my knowledge, the employee is authorized to work in the United States.			First Day of Employment (mm/dd/yyyy):	
Last Name, First Name and Title of Employer or Authorized Representative		Signature of Employer or Authorized Representative		Today's Date (mm/dd/yyyy)
Employer's Business or Organization Name		Employer's Business or Organization Address, City or Town, State, ZIP Code		

For reverification or rehire, complete Supplement B, Reverification and Rehire on Page 4.

City of Medford Computer Use Policy

General Information

This policy serves to protect the security and integrity of the City's electronic communication and information systems by educating employees about appropriate and safe use of available technology resources.

Computers and related equipment used by City employees are property of the City. The City reserves the right to inspect, without notice, all data, emails, files, settings, or any other aspect of a City-owned computer or related system, including personal information created or maintained by an employee. The City may conduct inspections on an as-needed basis as determined by the City Administrator or designee.

Beyond this policy, the City Administrator or designee may distribute information regarding precautions and actions needed to protect City systems; all employees are responsible for reading and following the guidance and directives in these communications.

Personal Use

The City recognizes that some personal use of City-owned computers and related equipment has and will continue to occur. Some controls are necessary, however, to protect the City's equipment and computer network and to prevent abuse of this privilege.

Reasonable, incidental personal use of City computers and software (e.g., word processing, spreadsheets, email, Internet, etc.) is allowed but should never preempt or interfere with work. All use of City computers and software, including personal use, must adhere to provisions in this policy, including the following:

- Employees shall not connect personal peripheral tools or equipment (such as printers, digital cameras, disks, USB drives, or flash cards) to City-owned systems, without prior approval from their supervisor. If permission to connect these tools/peripherals is granted, the employee must follow provided directions for protecting the City's computer network.
- Personal files should not be stored on City computer equipment. This also applies to personal media files, including but not limited to mp3 files, wav files, movie files, iTunes files, or any other file created by copying a music CD, DVD, or files from the Internet. Your supervisor will delete these types of files if found on the network, computers, or other City-owned equipment. Exceptions would be recordings for which the City has created, owns, purchased, or has a license.
- City equipment or technology shall not be used for personal business interests, for-profit ventures, political activities, or other uses deemed by your supervisor to be inconsistent with City activities. If there is any question about whether a use is appropriate, it should be forwarded to City Administrator or designee for a determination.

Hardware

In general, the City will provide the hardware required for an employee to perform his or her job duties. Requests for new or different equipment should be made to your supervisor, who will forward the request to the City Administrator or designee.

The City will not supply laptop computers based solely on the desire of employees to work offsite.

Only City staff may use City computer equipment. Use of City equipment by family members, friends, or others is prohibited.

Employees are responsible for the proper use and care of City-owned computer equipment. City computer equipment must be secured while off City premises; do not leave computer equipment in an unlocked vehicle or unattended at any offsite facility. Computer equipment should not be exposed to extreme temperature or humidity. If a computer is exposed to extreme heat, cold, or humidity, it should be allowed to achieve normal room temperature and humidity before being turned on.

Software

In general, the City will provide the software required for an employee to perform his or her job duties. Requests for new or different software should be made to your supervisor, who will forward the request to the City Administrator or designee.

Employees shall not download or install any software on their computer without the prior approval of their supervisor. Exceptions to this include updates to software such as Microsoft updates, Adobe Reader, and Adobe Flash. Your supervisor may, without notice, remove any unauthorized programs or software, equipment, downloads, or other resources.

Electronic Mail: The City provides employees with an email address for work-related use. Some personal use of the City email system by employees is allowed, provided it does not interfere with an employee's work and is consistent with all City policies.

Employee emails (including those that are personal in nature) may be considered public data for both e-discovery and information requests and may not be protected by privacy laws. Email may also be monitored as directed by the City authorized staff and without notice to the employee.

Employees must adhere to these email guidelines:

- Never transmit an email that you would not want your supervisor, other employees, members, city officials, or the media to read or publish (e.g., avoid gossip, personal information, swearing, etc.).
- Use caution or avoid corresponding by email on confidential communications (e.g., letters of reprimand, correspondence with attorneys, medical information).
- Do not open email attachments or links from an unknown sender. Delete junk or "spam" email without opening it if possible. Do not respond to unknown senders.
- Do not use harassing language (including sexually harassing language) or any other remarks, including insensitive language or derogatory, offensive, or insulting comments or jokes.

Electronic Calendars: A shared calendar environment may be provided as part of the City's email software program. If the shared calendar is provided and required, all employees are required to keep their electronic calendar up to date and, at a minimum, must grant all staff the ability to view their calendar.

Instant Messaging: Due to data retention concerns, the City does not provide employees with resources or tools to communicate by instant messaging (IM) when conducting City business. Employees are not allowed to use IM as a mechanism for personal communication through the City's computer network or when using City equipment, and are not allowed to download or install any IM software on their City computer.

Personal Devices: Employees may choose to use their own equipment to read or compose email or other City data as governed in this policy. Employees understand that by connecting their personal equipment to the City's email server, their personal devices could be searched during an e-discovery or other court-ordered scenarios, and agree to grant access to their personal devices should such a situation arise.

Security

Passwords: Employees are responsible for maintaining and securing computer/network passwords.

Network access: Non-City-owned computer equipment used in the City's building should only use the wireless connection to the Internet. Under no circumstances should any non-City-owned equipment be connected to the City's computer network via a network cable. Exceptions may be granted by the City Administrator or designee.

Personal computer equipment may not be connected to the City's network without prior approval of your supervisor. Personal equipment may be subject to password requirements or other electronic security measures as determined by your supervisor.

Remote Access to the Network: Examples of remote access include, but are not limited to: Outlook Web Access (web mail), virtual private network (VPN), Windows Remote Desktop, and Windows Terminal Server connections. While connected to City computer resources remotely, all aspects of the City's Computer Use Policy will apply, including the following:

- With the exception of Outlook Web Access, remote access to the City's network requires a request from a supervisor.
- Remote access privileges may be revoked at any time by an employee's supervisor.
- If remote access is from a non-City-owned computer, updated anti-virus software must be installed and operational on the computer equipment, and all critical operating system updates must be installed prior to connecting to the City network remotely. Failure to comply could result in the termination of remote access privileges.
- Recreational use of remote connections to the City's network is strictly forbidden. An example of this would be a family member utilizing the City's cellular connection to visit websites.
- Private or confidential data should not be transmitted over an unsecured wireless connection. Wireless connections are not secure and could pose a security risk if used to transmit City passwords or private data while connecting to City resources. Wireless connections include those over cellular networks and wireless access points, regardless of the technology used to connect.

Internet

The following considerations apply to all uses of the Internet:

- Information found on the Internet and used for City work must be verified to be accurate and factually correct.
- Reasonable personal use of the Internet is permitted. Employees may not at any time access inappropriate sites. Some examples of inappropriate sites include but are not limited to adult entertainment, sexually explicit material, or material advocating intolerance of other people, races, or religions. If you are unsure whether a site may include inappropriate information, you should not visit it.
- If an employee's use of the Internet is compromising the integrity of the City's network, your supervisor may temporarily restrict that employee's access to the Internet. If your supervisor does restrict access, they will notify the employee, and the City Administrator as soon as possible, and work with the employee and manager to rectify the situation.
- The City may monitor or restrict any employee's use of the Internet without prior notice, as deemed appropriate by the employee's supervisor in consultation with the Administrator.

Data Retention

Electronic data should be stored and retained in accordance with the City's records retention schedule.

Storing and Transferring Files: If you are unsure whether an email or other file is a government record for purposes of records retention laws or whether it is considered protected or private, check with your supervisor. If you are unsure how to create an appropriate file structure for saving and storing electronic information, contact the City Administrator or designee.

Employees must adhere to these guidelines when transferring and storing electronic files:

- All electronic files must be stored on network drives. The City will not back up documents stored on local computer hard drives, and holds no responsibility for recovery of documents on local computer hard drives should they fail. Files may be temporarily stored on a laptop hard drive when an employee is traveling/offsite; however, the files should be copied to network as soon as possible.
- Electronic files, including emails and business-related materials created on an employee's home or personal computer for City business, must be transferred to and stored on the City's network. City-related files should not be stored on an employee's personal computer, unless otherwise defined in this policy.
- All removable storage media (e.g., CD-ROM, flash or USB drive, or other storage media) must be verified to be virus-free before being connected to City equipment.
- Email that constitutes an official record of City business must be kept in accordance with all records retention requirements for the department and should be copied to the network for storage.
- Email that is simple correspondence and not an official record of City business should be deleted (from both the "Inbox" and the "Deleted" box) as soon as possible and should not be retained by employees for more than three months. The City will not retain emails longer than one year on the network or in network back-ups.
- Electronic files or emails that may be classified as protected or private information should be stored in a location on the City's network that is properly secured.
- Any files considered private or confidential should not be stored anywhere other than the City's network. If there is a need to take confidential information offsite, it must be stored on encrypted media.

Employee signature

I have received and read the above policy and have had an opportunity to ask any questions. I understand that my failure to follow this policy may result in disciplinary action, including revocation of system privileges or disciplinary action, including but not limited to termination of employment.

_____ (Print Employee Name)

_____ (Employee Signature)

_____ (Print Department Name)

_____ (Date)

City of Medford Social Media Policy

Purpose

Social networking in government serves two primary functions: to communicate and deliver messages directly to citizens and to encourage citizen involvement, interaction, and feedback. Information which is distributed via social networking must be accurate, consistent, and timely and meet the information needs of the City's customers. Since social media is used for social networking, this policy seeks to ensure proper use of the City of Medford's social media sites by its representatives.

The City of Medford wishes to establish a positive and informative social media presence. City representatives have the responsibility to use the City's social media resources in an efficient, effective, ethical and lawful manner pursuant to all existing City and departmental policies. This policy also provides guidelines and standards for city representatives regarding the use of social media for communication with residents, colleagues and all other followers.

Policy

The City of Medford will determine, at its discretion, how its web-based social media resources will be designed, implemented and managed as part of its overall communication and information sharing strategy. City social media sites may be modified or removed by the City at any time and without notice, as described in this document. The city administrator shall be designated as the person with authority to monitor social media and insure compliance.

City of Medford social media accounts are considered a City asset and administrator access to these accounts must be securely administered. The City reserves the right to shut down any of its social media sites or accounts for any reason without notice.

All social media web sites created and utilized during the course and scope of an employee's performance of his/her job duties will be identified as belonging to the City of Medford, including a link to the City's official web site.

Scope

This policy applies to any existing or proposed social media web sites sponsored, established, registered or authorized by the City of Medford. This policy also covers the private use of the City's social media accounts by all City representatives, including its employees and agents, Council members, appointed board or commission members and all public safety volunteers to the extent it affects the City. Questions regarding the scope of this policy should be directed to the City Administrator.

Definition

Social media are internet and mobile-based applications, websites and functions, other than email, for sharing and discussing information, where users can post photos, video, comments and links to other information to create content on any imaginable topic. This may be referred to as "user-generated content" or "consumer-generated media."

Social media includes, but is not limited to:

- Social networking sites such as Facebook, LinkedIn, Twitter, and online dating services/mobile apps
- Blogs
- Social news sites such as Reddit and BuzzFeed
- Video and photo sharing sites such as YouTube, Instagram, SnapChat, and Flickr
- Wikis, or shared encyclopedias such as Wikipedia
- An ever emerging list of new web-based platforms generally regarded as social media or having many of the same functions as those listed above

As used in this policy, “employees and agents” means all City representatives, including its employees and other agents of the city, such as independent contractors or Council members.

Rules of Use

City employees and agents with administrator access are responsible for managing social media websites. Facilities or departments wishing to have a new social media presence must initially submit a request to the City Administrator in order to ensure social media accounts are kept to a sustainable number and policies are followed. All approved sites will be clearly marked as the City of Medford site and will be linked with the official City website (www.medfordminnesota.com). No one may establish social media accounts or websites on behalf of the City unless authorized in accordance with this policy

Administration of all social media web sites must comply with applicable laws, regulations, and policies as well as proper business etiquette. The city administrator shall be designated as the person with authority to monitor social media and insure compliance.

City social media accounts accessed and utilized during the course and scope of an employee’s performance of his/her job duties may not be used for private or personal purposes or for the purpose of expressing private or personal views on personal, political or policy issues or to express personal views or concerns pertaining to City employment relations matters.

No social media website may be used by the City or any City employee or agent to disclose private or confidential information. No social media web site should be used to disclose sensitive information; if there is any question as to whether information is private, confidential or sensitive, contact the City Administrator.

When using social media sites as a representative of the City, employees and agents will act in a professional manner. Examples include but are not limited to:

- Adhere to all City personnel policies
- Use only appropriate language

Be aware that content will not only reflect on the writer but also on the City of Medford as a whole, including elected officials and other city employees and agents. Make sure information is accurate and free of grammatical errors.

- Not providing private or confidential information, including names, or using such material as part of any content added to a site.
- Not negatively commenting on community partners or their services, or using such material as part of any content added to a site.
- Not providing information related to pending decisions that would compromise negotiations.
- Be aware that all content added to a site is subject to open records/right to know laws and discovery in legal cases.
- Always keep in mind the appropriateness of content.
- Comply with any existing code of ethical behavior established by the City.

Where moderation of comments is an available option, comments from the public will be moderated by City staff, with administrative rights, before posting. Where moderation prior to posting is not an option, sites will be regularly monitored by City staff.

City of Medford's staff with administrative rights will not edit any posted comments. However, comments posted by members of the public will be removed if they are abusive, obscene, defamatory, in violation of the copyright, trademark right or other intellectual property right of any third party, or otherwise inappropriate or incorrect. The following are examples of content that may be removed by City staff before or shortly after being published:

- Potentially libelous comments
- Obscene or racist comments
- Personal attacks, insults, or threatening language
- Plagiarized material
- Private, personal information published without consent
- Comments totally unrelated to the topic of the forum
- Commercial promotions or spam
- Hyperlinks to material that is not directly related to the discussion

Personal Social Media Use

The City of Medford respects employees and agents' rights to post and maintain personal websites, blogs and social media pages and to use and enjoy social media on their own personal devices during non-work hours. The City requires employees and agents to act in a prudent manner with regard to website and internet postings that reference the City of Medford, its personnel, its operation or its property. Employees and agents and others affiliated with the City may not use a city brand, logo or other city identifiers on their personal sites, nor post information that purports to be the position of the City without prior authorization.

City employees and agents are discouraged from identifying themselves as city employees when responding to or commenting on blogs with personal opinions or views. If an employee chooses to identify him or herself as a City of Medford employee, and posts a statement on a matter related to City business, a disclaimer similar to the following must be used:

"These are my own opinions and do not represent those of the City."

There may be times when personal use of social media (even if it is off-duty or using the employee's own equipment) may spill over into the workplace and become the basis for employee coaching or discipline. Examples of situations where this might occur include:

- Friendships, dating or romance between co-workers
- Cyber-bullying, stalking or harassment
- Release of confidential or private data; if there are questions about what constitute confidential or private data, contact the City Administrator.
- Unlawful activities
- Misuse of city-owned social media
- Inappropriate use of the city's name, logo or the employee's position or title
- Using city-owned equipment or city-time for extensive personal social media use

Each situation will be evaluated on a case-by-case basis because the laws in this area are complex. If you have any questions about what types of activities might result in discipline, please discuss the type of usage with the City Administrator.

Data Ownership

All social media communications or messages composed, sent, or received on city equipment in an official capacity are the property of the City and will be subject to the Minnesota Government Data Practices Act. This law classifies certain information as available to the public upon request. The City of Medford also maintains the sole property rights to any image, video or audio captured while a City employee is representing the City in any capacity.

The City retains the right to monitor employee's social media use on city equipment and will exercise its right as necessary. Users should have no expectation of privacy. Social media is not a secure means of communication.

Policy Violations

Violations of the Policy will subject the employee to disciplinary action up to and including discharge from employment.

I have reviewed and agree to follow the policy in its entirety.

Printed Name

Signature

Date

BLOODBORNE PATHOGENS
29 CFR 1910.1030

Employee Name(s): _____

Occupation: _____

Date: _____

In accordance with 29 CFR 1910.1030, I certify by my signature, that I have been provided with training that consisted of but was not limited to the following:

1. Explanation of the standard.
2. Identification of epidemiology and symptoms of Bloodborne pathogens.
3. Identification of modes of transmission
4. Exposure Control Plan-how to obtain a copy
5. Use and limitations of engineering controls, work practices and PPE
6. PPE - types use, location, removal, handling, decontamination, and disposal.
7. PPE- the basis for selection
8. Hepatitis B Vaccine
9. Emergency procedures - for blood and other potentially infectious materials.
10. Exposure incident procedures.
11. Post-exposure evaluation and follow-up
12. Signs and labels.

I understand that this training is mandatory, I will attend at least annually and will follow the safety policies and procedures in force.

EMPLOYEE SIGNATURE(S):

Employee Medical File Form
Hepatitis B Vaccination Status

Name: _____ Date Employed: _____

Date of Initial Infection Control Training: _____

Date HBV Vaccination education information given to employee: _____

Date HBV Vaccination series offered to employee: _____

Employee received HBV Vaccinations:

_____ No If employee refuses vaccinations, he or she shall sign declination statement.

If employee did not receive HBV vaccination for any other reason,
Explain:

_____ Yes, free of charge. If yes, record dates of injections.

Employee's Initials: 1st _____ 2nd _____ 3rd _____

Hepatitis B Vaccine Declination

I understand that due to my occupational exposure to blood or other potentially infectious materials I may be at risk of acquiring hepatitis B virus (HBV) infection. I have been given the opportunity to be vaccinated with hepatitis B vaccine, at no charge to myself. However, I decline hepatitis B vaccination at this time. I understand that by declining this vaccine, I continue to be at risk of acquiring hepatitis B, a serious disease. If in the future I continue to have occupational exposure to blood or other potentially infectious materials and I want to be vaccinated with hepatitis B vaccine, I can receive the vaccination series at no charge to me. Federal Register Vol. No. 235, Part 1910 of title 29, Section 1910.1030, pg 64182.

Employee Signature: _____ Date: _____

Employee now chooses to receive HBV Vaccinations, at no charge, after originally declining:

Record dates of injections:

1st _____ 2nd _____ 3rd _____
Employee's Initials: _____

Medical Information Release Form

I, _____ (full name of worker/
Patient), hereby authorize: _____ (individual or
organization holding medical records), to release to _____
(individual or organization, name and address, authorized to _____
receive the medical information), the following medical information from my personal
medical records:

But I do not give permission for any other use or re-disclosure of this information. (Note: Several extra lines are provided below so that you can place additional restrictions on this authorization letter if you want to. You may, however, leave these lines blank. On the other hand you may want to (1) specify a particular expiration date for this letter (if less than one year); (2) describe medical information to be created in the future that you intend to be covered by this authorization letter; or (3) describe portions of the medical information in your records which you do not intend to be released as a result of this letter.)

Full name of Employee or Legal Representative: _____

Signature of Employee or Legal Representative: _____

Date: _____

Signature of Witness: _____ Date: _____

Source: Appendix A to 1910.20 Access to employee exposure and medical records. Section 8 of the Occupational Safety and Health Act, 29 U.S.C. 657; Secretary of Labor's Order No. 9-83 (48 FR 35736) and 29 CFR part 1911.