

Information Technology Use Policy

Adopted May 20, 2020 by Administrative Order 2020-04
Amended Feb 4, 2021 by Administrative Order 2021-03

Information Technology Use Policy

Information Technology (IT) is a critical mechanism for operations and business communications at the City of Bozeman (City).

The purpose of this Information Technology Use Policy is to outline appropriate and inappropriate use of the City's IT systems and services to improve efficiencies and minimize disruptions to services and activities, as well as comply with applicable policies and laws. All department directors, supervisors, employees, and officials with access to the City's network are required to comply with this Policy. Failure to comply for employees may result in disciplinary action up to and including termination of employment. *See* Section 10.

Scope

This Policy applies to all Internet, hardware, software applications, computers, cell phones, and email systems owned or operated by the City. All users of any City system must abide by this Policy. This Policy includes the appendices listed in the table of contents, which are incorporated in the Policy by this reference.

The term "computer" utilized in this Policy (unless otherwise specified) includes, but is not limited to, desktop computers, laptop computers, tablets, and other similar devices.

The term "cell phone" utilized in this Policy (unless otherwise specified) includes, but is not limited to, smartphones, flip phones, and other similar devices.

The City complies with all applicable federal, state, and local laws as they concern the employer/employee relationship. Nothing contained herein is intended to or should be misconstrued to violate any of the rights or responsibilities contained in such laws.

Table of Contents

Information Technology Use Policy.....	1
Information Technology Use Policy.....	2
Section 1. Account Activation/Termination	4
Section 2. Password Guidelines.....	5
Section 3. Expectations for Use of all IT Systems	5
Section 4. City Email Use	7
Section 5. Internet Use Expectations	8
Section 6. Cell Phone Use	9
Section 7. Monitoring and Confidentiality	11
Section 8. Reporting Misuse.....	12
Section 9. Disclaimer	12
Section 10. Failure to Comply.....	13
Section 11. Appendices	13
Appendix A-Social Media Use.....	13
Appendix B-Cloud Services	22
Appendix C-Web Governance.....	25
Recognition and Acceptance of both the City IT Use Policy.....	30
Employee Verification of Compliance with Sections 3.4, 6.6, and 6.7 Upon Return of Computer or Cell Phone to IT Department.....	31

Section 1. Account Activation/Termination

1.1 System, internet, and email access at the City is controlled through individual accounts and passwords. Each user of the City's internet, network, email, and other systems, must read and sign a copy of this Policy prior to receiving internet, email or system access. It is the responsibility of each user to protect the confidentiality of their accounts and password information. Users must use their own username and password to log onto City computers and cell phones. Usernames and passwords must not be shared and are for the sole use of the person to whom they have been assigned. If multiple users are sharing the same city equipment, each user should log in with their own username and password. Exceptions to this practice may be approved by the IT Director. (Example: Computers at the front desk in the Finance Department that are used for taking payments and used by all billing clerks).

1.2 A user may access only the computers, computer accounts, and computer files for which the user has authorization.

1.3 A user may not access another individual's account, or attempt to capture or guess other users' passwords.

1.4 System and email accounts may be granted to third party non-employees on a case-by-case basis as approved by the IT Director. Non-employees that may be eligible for access include:

- City Board members;
- Contractors;
- Interns (paid/non paid); or
- Volunteers.

Requests for third party non-employee accounts must be submitted via email to the IT Director. All terms, conditions, and restrictions governing password, internet, email and systems use as specified in this Policy must be complied with by third party non-employees and a copy of this Policy must be signed by the user.

1.5 Systems, cell phone use, and email access will be terminated when the employee or third party terminates their association with the City, unless authorized by the IT Director.

1.6 The City is under no obligation to store or forward personal contents of an individual's email inbox/outbox or local hard drive after the ending of their association with the City. All correspondence and files are the property of the City and will be stored according to the City's records retention policy.

1.7 You are required to take reasonable steps to ensure any information saved on your computer and/or City-provided cell phone is saved on the network or other location in accordance with Sections 3.4, 6.6, and 6.7 herein prior to leaving the employment of the City and/or when otherwise terminating your use of the device. Each user must review the information stored on their computer(s) and cell phone(s) to ensure such data is also stored on a city network. The purpose of this review is to ensure all information has been saved to the network or other location as required by Sections 3.4, 6.6, and 6.7. After completion of your review, you will be asked to sign the form at the end of this Policy verifying you have taken reasonable steps to confirm your information has been saved to the network in conformance with Section 3.4., 6.6, and 6.7. If you have questions regarding how to review your computer or cell phone, please contact the IT Department for assistance. The IT Department may request a supervisor and/or other individual to conduct this review.

Section 2. Password Guidelines

2.1 Passwords are used to access City systems, including the network, email, the internet, and voicemail. Weak passwords place the entire system at risk. Therefore, strong passwords are required. Create a password that is also easy to remember. Never share your password. It is for your use and your use only. The City requires passwords be changed every 90 days. The IT Director may change this password policy to require the use of pass phrases. These pass phrases, if required, will have to be changed every 12 months unless security concerns arise that warrant a password change prior to the 12-month timeframe.

○

Section 3. Expectations for Use of all IT Systems

Appropriate Use

3.1 Employees and officials must use the internet and email systems responsibly, as unacceptable use can place the City and others at risk. The City expects individuals at the City to use City IT systems to further the goals and objectives of the City.

3.2 Activities that are encouraged include:

- communicating with fellow employees, business partners of the City, and public constituents within the context of an individual's assigned responsibilities;
- acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities;
- automation of tasks and processes to improve productivity and cooperation between departments;
- participating in educational or professional development activities.

Inappropriate Use

3.3 The City's IT systems and services must not be used for purposes that could be reasonably expected to cause excessive strain on systems. Individual email and internet use must not interfere with others' use of the City's email and internet system and services. All technology use at the City will comply with all applicable laws, including but not limited to Section 45-6-311, Montana Code Annotated, and the City's Ethics Code (chapter 2, article 3, and division 4 of the Bozeman Municipal Code). This Policy must be followed in conjunction with other City policies governing appropriate workplace conduct and behavior including but not limited to the City's Sexual Harassment Policy and City's Employee Handbook.

3.4 In addition to the expectations included in Sections 4, 5 and 6 below, the following activities are inappropriate uses of City IT systems and services and are prohibited:

- Use of IT systems for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal schemes, unauthorized downloads, and computer tampering (e.g. spreading of computer viruses);
- Uses of IT systems in any way that violates the City's policies, rules, or administrative orders;
- Viewing, copying, altering, or deletion of email and internet accounts or files belonging to the City or another individual without authorized permission (this includes any individuals leaving their current positions with the City);
- Disabling of protective services or software without IT Director's authorization;
- The use of non-City (personal) devices to produce City work product. The City of Bozeman does not currently support using your own (personal) devices for work functions, formally known as BYOD (Bring Your Own Device). This policy may change in the future as more issues related to wage and labor laws are resolved.
- Connecting non-City (personal) devices to City networks -only the BozemanGuest WiFi may be used for connecting non-city (personal) devices.
- The storage of City work product on local devices or personal devices unless otherwise authorized. City work product must be stored in the appropriate network, authorized software application, or authorized cloud location. The purpose of this requirement is to enable legal discovery, ensure compliance with records retention requirements, and provide for backup and data loss prevention should a local device fail.
- In accordance with the City's Purchasing Policy, the purchase of hardware or software must be approved by the IT Director prior to purchase.
- Entering into technology related contracts without involvement of the City Attorney's Office and IT Department. This includes software licenses and agreements.
- Use of outside IT groups to perform IT related work without approval of the IT Director.

- Sending of unreasonably large email attachments. The total size of individual email messages sent (including attachment) should be 25MB or less.
- Opening email attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution;
- Sharing email and internet account passwords with another person, or attempting to obtain another person’s email and internet account password. Email and internet accounts are to be used by the registered user only.
- Excessive personal use of the City’s IT Systems. The City allows limited personal use of Internet services and email services for communication with family and friends, independent learning, and public service provided such use does not interfere with staff productivity, pre-empt any business activity or consume more than a minimal amount of resources. The City prohibits personal use of its email systems and services for unsolicited mass mailings, non-City commercial activity, political campaigning, promoting or opposing a candidate or ballot issue, dissemination of chain letters and use by non-employees.

Section 4. City Email Use

Email is a critical tool for City communications. This section applies to all email systems managed by the City, all email account users and all City email records.

- 4.1 Official communications are often delivered via email. Employees with City email accounts are expected to check their email in a consistent and timely manner so that they are aware of important organizational announcements and updates, and can fulfill City tasks. If employees are unable to check their mail for an extended period, they should use the “automatic reply” (Out of Office) feature. In certain circumstances, a department director may, in coordination with the assistance of the IT Department, authorize arrangements to have an employee’s email monitored by their supervisor and reviewed for messages needing a response.
- 4.2 All time spent by nonexempt employees using electronic communications for work purposes will be considered hours worked. Therefore, to avoid incurring unnecessary expenses, electronic communications must not be used outside regularly scheduled work hours. Nonexempt employees must not check for, read, send or respond to work-related emails outside their normal work schedules unless specifically authorized by their department director.
- 4.3 Email users are responsible for mailbox management, including organization, size management and periodic cleaning. If a user subscribes to a mailing list, he or she must be aware of how to remove him/herself from the list, and is responsible for doing so in the event that their current email address changes.

- 4.4 Email users should, when possible, send a link to documents they wish to share with other City users as opposed to adding the file as an attachment. This works well when sharing files that are on the projects, public, departmental or other mapped drives. This saves storage space in the email system.
- 4.5 Email users must have an accurate and detailed description of the subject of the email in the subject line. Email users must refrain from changing subjects/topics during an email chain. If a new subject is to be discussed a new chain must be created. All email recipients that need to act on an email should be included on the “To” line. Any recipients that you are including as an FYI to them should go on the “Cc” or “Bcc” lines. All users must have a signature block consisting of their name, title and contact information. The IT Department will stamp each email with the approved compliance language per MCA for all email users. The use of attachments in a signature line is prohibited. City logos in signature lines must be imbedded in the signature. For help with this please contact the IT Department.
- 4.6 City emails are generally considered public records and subject to the Montana Open Records Act. You agree you have no reasonable expectation of privacy in your City email account. Officials and employees should avoid using City email accounts for personal communications. Employees or officials wishing to maintain privacy in their personal email communications must use a personal email account for those communications. All incoming and outgoing City emails are archived for records retention purposes.
- 4.7 Email users are not authorized to use personal email accounts (i.e. Gmail, Hotmail, etc.) for conducting city business. Microsoft Outlook must be used for all city email communications.
- 4.8 Email users must also understand emails may be searched for and reviewed during review of claims or in litigation where the City, its employees, officials, or agencies are a party, to respond to requests for public information, and in circumstances where such a search and review has been authorized by the City Manager. Although the City Attorney’s Office will generally seek to protect a user’s privacy where legally required, emails containing private or sensitive information may be released without notice to the account holder. Emails that violate this Policy may be forwarded to the employee’s department director for review in compliance with Sections 7 and 10, below.
- 4.9 The authority to send an email to all City email users is limited to the City Manager (or their designee), Assistant City Managers, IT Director, IT Department Systems Administrators and the HR Director.

Section 5. Internet Use Expectations

- 5.1 All authorized users of the City’s internet resources, including the World Wide Web, intranet, FTP (File Transfer Protocol), IM (Instant Messaging), etc. must comply with this Policy. The City makes the internet available for officials and employees as a tool to facilitate the effective operation of City

government. Limited personal use of the City's network that does not interfere with City work is authorized. However, all users agree they have no expectation of privacy in the contents or search histories of such internet use. Users wishing to maintain privacy in their personal internet use must use a personal device and network.

5.2 Inappropriate use of the City provided internet includes, but is not limited to:

- Sending or posting discriminatory, harassing, or threatening messages or images on the internet or via the City's email services.
- Using City internet to perpetrate any form of fraud, and/or software, film, or music piracy.
- Sharing confidential material or proprietary information outside of the City.
- Hacking activities of any kind.
- Downloading unauthorized software, or using unauthorized software, either online or local, for City work purposes.
- Using the City's networks or email to support or oppose a candidate for elected public office or a ballot measure.

5.3 The social media use policy (Appendix A) applies to all employees, volunteers, interns, contractors, City board members and City elected officials.

5.4 Employees are prohibited from posting, transmitting and/or disseminating any City-owned photographs, video or audio recordings, likeness or images or departmental logos, emblems, uniforms, badges, patches, marked vehicles, equipment, or other materials that specifically identifies the City on any personal or social media website or web page, without the permission of the IT Director.

Section 6. Cell Phone Use/Chat Messaging

6.1 The City issues cell phones to employees who need them to do their job. Doing so increases the efficiency and safety of City operations. The City benefits by:

- redundancy of communication capabilities: when landlines fail, key employees are already carrying cell phones with data service. This can be critical for saving lives and resources in public safety and public works emergencies;
- allows contact with public safety and other key employees who may need to be reached outside of normal business hours.
- enables employees to complete work and correspondence while away from their desks, during the employee's customary hours of work; and
- enables employees authorized by their department director to complete work and correspondence remotely if needed.

6.2 All time spent by nonexempt employees using cell phones for work purposes will be considered hours worked. Therefore, to avoid incurring unnecessary expenses, cell phones should not be used for City purposes outside regularly scheduled work hours unless authorized by the employee's department director. Nonexempt employees should not make or respond to work-related communications outside their normal work schedules unless specifically authorized by their department director. In the event a non-exempt employee does respond to work-related communications outside of normal work schedules, the time must be reported.

6.3 Service Agreements – The City will provide a service agreement sufficient to cover all City business-related communication (calls, data and text) on City-issued cell phones. The IT Department is responsible for enrolling individual accounts in the appropriate service plan after consultation with the appropriate department director. No employee may independently contract for City cell phone service on their own. The IT Department will conduct a review of all service agreements every twelve months. The IT Department will make changes to agreements to ensure that accounts are not “over” or “under” subscribed for City-related activity at that time.

On a monthly basis, the IT Department will review the cellular bill. Any billing concerns will be brought to the attention of the appropriate Finance Department staff for resolution.

6.4 Personal Use – City-provided devices will only be issued when it is in the best interest of the City to do so. Employees who are assigned to carry a city-provided phone or data device may use the device for limited personal use. When an employee or official uses a cell phone for personal use the employee or official specifically recognizes any privacy interests in the contents, the sender, or the recipients of any data transferred via the device is greatly reduced. This includes text messages or other messaging. Employees wishing to maintain complete privacy in their personal communications must use a personal device for those communications.

6.5 Device Purchases & Replacements – The IT Department will determine when a cell phone needs replacement. The IT Department will purchase, set-up and service the cell phone. The cost of the new cell phone will be charged to the benefitting employee's department.

6.6 Text Messaging

- Employees with City-provided cell phones may use text messaging only for routine or transitory messages where the applicable record retention schedules would not potentially require the message to be retained for longer than 30 days. Text messaging for City business is prohibited on non-City-provided cell phones.
- If an employee receives or inadvertently sends a text message that needs to be retained for longer than 30 days pursuant to a record retention schedule, legal hold, or otherwise, it is the responsibility of the employee to contact the IT Department for the purpose of having the

text message preserved. Otherwise, the employee should delete routine or transitory text messages in accordance with the records retention schedule(s).

- Employees with City-provided cell phones may not use any other types of messaging for City business, other than the text message application, that comes with the phone.
- Employees are encouraged to communicate this requirement to non-City individuals and entities to ensure all non-routine communications occur through email or other methods capable of complying with this Policy.

6.7 Photographs

Photographs taken on City-owned cell phones for City business must be preserved in accordance with the applicable record retention schedules. Pictures taken should be saved to the network as soon as possible after they have been taken. Please contact the IT Department with respect to how to preserve photographs taken on City-owned cell phones.

6.8 Chat Messaging

- Employees with City-provided cell phones may use Microsoft Teams Chat Messaging only for routine or transitory messages where the applicable record retention schedules would not require the message to be retained for longer than 30 days. Use of Teams is only permitted after Teams training has been assigned and completed by the user in the Learning Management System.
- If an employee receives or inadvertently sends a chat message that must be retained for longer than 30 days pursuant to a record retention schedule, legal hold, or otherwise, it is the responsibility of the employee to immediately contact the IT Department for the purpose of having the chat message preserved.
- Employees may not use any other types of chat messaging for City business, other than Microsoft Teams chat that is connected to the City's Microsoft Office 365 environment.
- Employees must communicate this requirement to non-City individuals and entities to ensure all non-routine communications occur through email or other methods capable of complying with this Policy.

Section 7. Monitoring and Confidentiality

7.1 City computers, cellphones and the IT systems and services used at the City are owned by the City and not the employees or officials who use them. The use of these computers, cellphones, systems and services by an employee means the employee understands such use is not private. The City reserves the right to monitor, examine, and regulate all email, messaging, or internet traffic passing through or stored on its email and internet systems. While the IT Department does not actively read

end-user email or messaging, email messages may be inadvertently read by IT staff during the normal course of managing the email/messaging system or by staff of the City Attorney's Office and other city employees in the normal course of records requests, personnel actions, or claims and litigation.

7.2 In addition, backup copies of email messages or other messaging data may exist, despite end-user deletion, in order to comply with the City's records retention and legal hold policies. The goals of these backup and archiving procedures are to ensure system reliability, prevent business data loss, and comply with applicable laws.

7.3 If the City discovers, or has good reason to suspect an employee's or official's email or internet activities do not comply with applicable laws or this Policy, the City may retrieve and use any email, messaging and internet records in any legal or disciplinary action. Only the City Manager or the City Attorney may authorize a review of an official's or employee's email, messaging, or internet records and only a director of the employee's department, the City Manager, and/or the City Attorney or their designees, as appropriate, may review an email account or internet activity.

7.4 Employees must use extreme caution when communicating confidential or sensitive information via email and internet systems. Keep in mind that all email messages sent outside of the City become the property of the receiver. A good rule is to avoid communicating anything that you would not feel comfortable being made public. Demonstrate particular care when using the "Reply" or "Reply All" command during email correspondence.

7.5 Email that contains legally privileged or confidential information may not be distributed outside the City except as authorized by the City Attorney or City Manager. Do not forward an email or email chain which includes email(s) to or from a city attorney, or questions to or advice from a city attorney, without first obtaining permission from a city attorney.

Section 8. Reporting Misuse

8.1 Allegations of misuse must be promptly reported to the person's immediate supervisor. Supervisors must report the allegation to the IT Director.

8.2 If you receive an offensive email, do not forward, delete, or reply to the message. Instead, report it directly to your immediate supervisor. Supervisors should report it to the IT Department via telephone before taking any additional action.

Section 9. Disclaimer

The City assumes no liability arising from the unauthorized use of the City's email and/or internet systems and services. Users are solely responsible for the unauthorized content they disseminate. The

City is not responsible for any third-party claim, demand, or damage arising out of unauthorized use of the City's email systems or services.

Section 10. Failure to Comply

10.1 Any employee who violates any provision of this Policy may be denied future access to City-provided email and/or internet systems and, if appropriate, may be subject to disciplinary action up to and including termination, in accordance with the disciplinary procedures set out in the Employee Handbook.

Violation by an official, board or committee may subject the official(s) to sanction or removal.

10.2 Questions regarding the appropriate use of the City's computers, cell phones, network, or IT systems, including email and the internet, should be directed to your supervisor or the IT department.

Section 11. Appendices

Appendix A-Social Media Use

Social Media Use Policy

Section 1. Purpose

The City of Bozeman has established a social media presence to reach a broader audience of citizens, community members, and visitors with information about City services and events. To address the fast-changing landscape of communications, City departments, boards, and committees are authorized and encouraged to consider using social media tools to reach citizens and customers. Used carefully, in partnership with the City's IT Department and the communications coordinator these new communication channels can effectively further the missions and goals of the Strategic Plan.

Just as with any written communications of the City, we seek to ensure the City's social media communication presence is secure, that fair and open public discourse is able to occur, that these communications are properly archived, and that we foster an "all are welcome" forum for our citizens.

The City's use of social media currently falls into three general categories:

1. Disseminating time-sensitive information as quickly as possible (for example, releasing information related to an emergency);
2. Reaching a broad audience of citizens, community members, and visitors with information about our services, projects, and events. This usually entails the use of features such as gathering “followers” and “liking” other members of the online community;
3. Gathering input on City services and events from community members, citizens, or visitors.

Section 2. Applicability

This Policy applies to the development and ongoing use of City-owned websites, social media channels, and intranet portals. This policy also applies when an employee, contractor, or official uses non-city social media channels for city business within the scope of their duties as a City of Bozeman employee, contractor, or official.

This Policy applies to city boards and committees and to individual elected officials only upon the City Manager signing the Administrative Order. Boards, agencies, or committees shall have an assigned city staff member who is responsible for the management of the respective social media channels to ensure compliance with this Policy.

This Policy does not apply to an individual employee or official’s personal use of social media. Such use, however, may be governed by the City’s Information Technology Use Policy and other City policies, such as the Employee Handbook and the City’s Code of Ethics.

Unless made applicable to the City Commissioners by Commission resolution, this Policy shall not apply to an elected official’s social media pages. The City is not responsible for an elected official’s use of their own social media. An elected official should refrain from using their personal social media for official city business. City-sponsored accounts may not be used for election purposes.

Section 3. General

1. An employee, department, board, or committee may not create a social media channel on behalf of the City without the authorization and assistance of the IT Department and following all aspects of this Policy.
 - a. In order to maintain a coordinated web and social media presence for the City, the IT Department, Communications Coordinator, and department social media editors, will maintain appropriate links between the www.bozeman.net website and the various social media channels.
 - b. The IT Department will maintain a list of social media tools that are approved for use by City employees, departments, boards, and committees.

- c. Unless otherwise approved by the City Manager and IT Director, the IT Department shall be the sole entity authorized to construct and maintain the technical aspects (i.e., channel name, bozeman.net associations, permissions, assigned administrators, etc.) of all social media channels.
 - d. The IT Department will maintain a list of all City social media channel authorized administrators and other critical information required to assist in the administration of each channel. Each individual social media channel must have an employee of the IT Department listed as an administrator.
 - e. Departments, boards and committees must inform the IT Department of its interest in any new social media channels or changes to existing channels prior to the IT Department creating a new channel or modifying an existing channel. All new social media tools, such as a new social media channel, platform, or software application proposed for City employee, department, or board use must be approved by the City's IT Director.
 - f. The IT Department and the Communications Coordinator shall be responsible to provide social media training to employees, departments, boards, and committees as needed.
2. Daily management of content on a social media site shall be the responsibility of the employee, department, board, or committee authorized to manage a social media site.
 - a. Department directors are responsible for ensuring all social media use by their departments complies with this Policy.
 - b. City Boards and Committees are responsible for ensuring all social media use by their members complies with this Policy. A City board or committee desiring to use social media must do so in conformance with established rules of procedures and the decision to use social media must be entered into the minutes. Boards and Committees are expected to take special care to ensure that open meeting laws are not violated through the use of discourse on social media channels.
 - c. If a department, board, or committee utilizes a third-party contractor for any level of social media work, upon approval of the IT Director, the department responsible for the channel must ensure the contractor complies with this Policy.
 - d. A social media channel shall not be used for internal department work product. Doing so subjects the City to unnecessary risk of loss of information, inaccessibility to work product for other employees, and failed back-ups.
 - e. Required Training: No employee, department, board, or committee will participate in or administer a City social media channel without fulfilling the training requirements established by the IT Director and Communications Coordinator.
3. Social Media Channel Protocols will be established and updated as necessary by the IT Department. For each channel, these protocols identify the goal, channels used (URL's), assigned editors for moderating and administration (including IT staff), content (one-way or two-

way communication), app integration, photo/video use, likes/followers, and practice for removal of content, among others.

4. Existing Internet and Social Media: The City's principle website "www.bozeman.net" will remain the City's primary internet presence for all departments, boards, and committees. Policies related to the City's websites are included in Appendix C, Web Governance. The City currently allows and maintains the following social media platforms that are meant to augment and, where possible, link with the primary website. For a current list of Social Media Channels being used at the City, contact the IT department Web and social Media Specialist.
 - Facebook
 - Twitter
 - YouTube
 - LinkedIn
 - Next Door
 - Instagram
 - Vimeo
5. The IT Department collects IP addresses, browser information, web site visitation analyses, including activity on social media channels, and similar data as part of their regular server logs. The City uses this information in aggregate form to improve the reach and effectiveness of its web sites and social media channels.

Section 4. Standards of Conduct for City Employees, Contractors, and Officials

Employees, contractors, officials, and others authorized to maintain content on a City-owned or sponsored social media site must conform to the following standards of conduct:

1. Citizen and customer protection and respect are paramount.
2. We will use every effort to keep interactions factual and accurate.
3. We will strive for transparency, accuracy, and openness in all social media interactions.
4. We will provide links to credible sources of information to support our interactions, when possible.
5. We will publicly correct any information we have communicated that is later found to be in error.
6. We are honest about our relationships, opinions, and identity.
7. We respect the rules of the venue.
8. We will protect privacy and permissions and will not collect personal information posted by individuals without a compelling reason.

9. We will adhere to our own terms of Acceptable Use.

In addition, all City employees and officials authorized to use social media understand that the lines between public and private and between personal and professional are often blurred. By identifying yourself as a City employee or official, you are creating perceptions about your expertise and about the City by stakeholders, customers, business partners and the public. You must ensure all content is consistent with the City's core values and professional and ethical standards.

Section 5. Content Posted to Social Media Channels

Whenever possible, all content posted to City social media channels by a City employee, department, board, or committee must also be posted on the City's principle website.

Content posted to City social media channels must be approved by the department director or by others as delegated by a department director or, for a board or committee by the staff liaison or board/committee member authorized by the IT Director, prior to posting. All content posted must, to the greatest extent possible, direct users back to the City's principle website for in-depth information, forms, documents or online services. All comments posted to any City authorized social media channel are bound by the policies, rules and regulations for that particular social media tool.

No employee, official, board, or committee may disclose confidential, proprietary, or other information protected by law from disclosure.

All City content on social media channels must comply with the Acceptable Use of City Social Media Site (see Section 8, below) and all other appropriate City policies and standards, including but not limited to:

1. Information Technology Use Policy;
2. City Code of Ethics, including confidentiality requirements;
3. All laws governing privacy, trade secrets, and other confidential information;
4. Unlawful Use of a Computer, 45-6-311, MCA;
5. The Montana Criminal Justice Information Act;
6. Bozeman City Commission Resolution 4250 regarding discrimination;
7. Section 24.10.010 – 24.10.080, Bozeman Municipal Code (Unlawful Discrimination);
8. City Employee Handbook; and
9. Federal copyright laws, federal and Montana trademark and service mark laws.

To ensure against copyright infringement:

- Use only City-owned photos, videos, and other images on the City's website.
- Assume that visual content you find online is protected by copyright, and do not post it to the City's social media channels.

- The City may have a license to use visual content the City does not own – for example, certain visual content created by a consultant or other third party. Be sure to abide by any and all copyright license requirements, including attribution.
- If you are uncertain about whether the City owns certain visual content or has a license to use it, please contact the IT Director and the City Attorney’s Office.

Section 6. Public Comments

Users and visitors to City social media channels shall be notified that the purpose of the site is to serve as a mechanism for communication between City departments and the public. City social media site articles and comments containing any of the following content are prohibited:

1. City employees are prohibited from making comments promoting or opposing any person campaigning for election to a political office or ballot issue while on City time or using City resources.
2. Promotion or advertisement of a business or commercial enterprise or solicitation of commerce, including by sharing, reposting, or retweeting the advertisement. Merely using a “like” or “follow” feature does not constitute an advertisement or solicitation.
3. The use of profane, obscene, threatening or harassing language;
4. Personal attacks of any kind;
5. Comments that promotes, fosters, or perpetuates discrimination on the basis of race, color, religion, creed, sex, age, marital status, national origin, or actual or perceived sexual orientation, gender identity, or disability as well as any other category protected by federal, state, or local law;
6. Sexual content or links to sexual content;
7. Comments that violate the protected privacy interests of any person;
8. Comments advocating illegal activity;
9. Content that violates a legal ownership interest of any other party; and
10. Information that may compromise the safety or security of the public or public systems.

The City reserves the right to restrict or remove any content that is deemed in violation of this social media policy or any applicable law. Removal of citizen comments on social media is authorized only by the IT Director, the City Manager, Assistant City Managers, or the City Attorneys. Any content removed based on these guidelines must be retained, including the time, date and identity of the poster when available and only removed after the City Attorney has reviewed the content, determined the content violates this policy, and approved removal.

Likes & Followers: The City seeks to expand its social media presence and reach by using the “Like” and “Follow” features of various channels. By using these features, the City is not endorsing, promoting, or advertising any business or commercial enterprise.

Advertisements: The City may find advertising its social media channels via purchase of advertisements on other entity social media channels is necessary and appropriate. The City will not accept advertisements from other entities on its social media channels.

Security: The City must ensure the security of its data and technical infrastructure in light of the new uses, users, and technologies related to social media. Departments, boards, and committees must be aware the use of social media may provide an avenue to access the City’s network without authorization to damage the City’s network or acquire confidential information. Departments, boards, and committees must educate their employees or members about various attack strategies hackers use to gain access to networks, security protocols, and the care needed when disclosing information using social media.

EMPLOYEES, BOARDS, AND OFFICIALS USING SOCIAL MEDIA MUST ADHERE TO THE FOLLOWING BASIC REQUIREMENTS:

- Read the published privacy guidelines of the social media service being used and take the time to understand these guidelines. These documents will include the types of information the services will reveal or sell to other parties (including spammers). If the terms and conditions of these documents are vague or objectionable, consult with the IT Department before using the service.
- After you type your email address and password into the login page, make sure the “Remember me” check box is turned off before you click the log-in button.
- Do not allow your browser to save passwords.
- Always remember to log-out when finished using the Social Media site.
- Never use personally identifiable or private information on social media channels, such as social security numbers, financial or health care information, or information involving trade secrets or individual personnel matters.
- If a channel is vandalized, discontinue the channel immediately and notify the IT department. Indications that the site has been tampered with may include alteration or removal of site graphics or logos, changes to expected functionality, or unapproved content postings.
- Passwords to access social media channels must not be the same as the employee or official’s password to access bozeman.net.

Section 7. Public Records

Documents, media, and communications posted on a City social media site are subject to State of Montana public records laws and City policies and procedures regarding public information and record retention. Any content in a social media format that is related to City business, including a list of subscribers and posted communication, is considered public information. The employee, department, board, or committee maintaining a social media site is responsible for coordinating with the City Clerk's office for the management of public information and records and for responding completely and accurately to any public records and information requests for social media content. Content related to City business must be maintained in an accessible format and produced in a timely manner in response to a request for public information or records. Wherever possible, such sites shall clearly indicate that any articles and any other content posted or submitted for posting are subject to public disclosure.

Montana law and City records and information retention schedules apply to social media formats and social media content. Unless otherwise addressed in a specific social media standards document, a department and each board or committee, of the City maintaining a site shall preserve records and information pursuant to a relevant records retention schedule in a format that preserves the integrity of the original record or information and is readily accessible. Currently the City uses Pagefreezer to accomplish this for all Social Media Channels.

Section 8. Statement on Acceptable Use of City Social Media Channels

All employees, contractors, and officials maintaining a social media site shall inform the public of the City's required standards of acceptable use of its social media channels. To that end, the specific statement provided below must be included on all City social media channels.

Each employee, contractor, or official authorized to manage a social media channel is responsible for oversight of this Acceptable Use statement for their managed site(s). Questions regarding technical compliance with this Acceptable Use statement should be directed to the IT Director. Questions regarding whether to remove a post or comment should be directed to the City Attorney.

All City social media channels must include in a prominent location on the site a link, text box, or page that contains the following Acceptable Use Policy:

“Acceptable Use Policy: Communicating with the City through social media enables you to contact the City in a direct and meaningful way. If you wish to comment or post material on this site you do so with the understanding that you agree to this policy and its standards of use as an initial and ongoing condition of your use.

When engaging with the City of Bozeman through the City's social media channels, you agree to the following:

1. Every comment or posting you make to a City of Bozeman social media site is a public record and may be disseminated, reproduced, or copied by the City or any other person without any further action by the poster or without notice by the City of such. You agree you have no reasonable expectation of privacy in anything you post to a City social media site.
2. Comments must be directly related to the posted topic for the City's social media page or post. The City of Bozeman department and division social media accounts are not meant for comments that do not directly relate to the purpose or topic of the social media website or for service complaints. For general comments or communications concerning a department or division, please contact the department or division directly by phone or email.
3. Comments posted to these sites are monitored by City employees and, while comments will not be edited by the City, a comment (or an appropriate portion thereof) may be removed if it violates any part of this policy.
4. When you post you are subject to the policies, rules, and regulations (i.e. the Terms of Service (TOS)) of the host site. Information (photos, videos, etc.) you share with or post to official City of Bozeman department, division, board or committee pages is also subject to the TOS of the host site and may be used by the owners of the host site for their own purposes. For more information, consult the host website's TOS.
5. Comments containing any of the following forms of content shall not be allowed and may be removed by the City without notice to you:
 - a. Promotion or advertisement of a business or commercial enterprise or solicitation of commerce;
 - b. The use of profane, obscene, threatening or harassing language;
 - c. Personal attacks of any kind;
 - d. Comments that promotes, fosters, or perpetuates discrimination on the basis of race, color, religion, creed, sex, age, marital status, national origin, or actual or perceived sexual orientation, gender identity, or disability as well as any other category protected by federal, state, or local law;
 - e. Sexual content or links to sexual content;
 - f. Comments that violate the protected privacy interests of any person;
 - g. Comments advocating illegal activity;
 - h. Content that violates a legal ownership interest of any other party; and
 - i. Information that may compromise the safety or security of the public or public systems.

6. Users are welcome to submit or post content, including photographs and videos, to an official City site where the department, division, board or committee allows users to post content, the content meets the standards articulated in this Acceptable Use Policy and pertains to the subject of the social media site. Users may only post their own, original content. Reproduced or borrowed content that reasonably appears to violate third party rights will be removed.

Questions or concerns regarding the City of Bozeman’s social media activity, the City's social media policy and/or this Acceptable Use Policy should be sent to it@bozeman.net.

This comment policy is subject to amendment or modification at any time.

By commenting or posting material to any City social media site you agree that every time you visit this site or any other City internet site you will be bound by the terms of this Acceptable Use Policy.”

If a violation of this policy occurs, the content editor and/or supervisor will notify the IT Department or the City Attorney’s Office. Appropriate instruction will be provided through the City Attorney's Office on steps for documenting and removal of inappropriate comments.

Appendix B-Cloud Services

POLICY FOR CLOUD SERVICE AGREEMENTS

Section 1. Purpose

To provide guidance regarding the selection, purchase and use of cloud computing services.

1.1 GENERAL PROVISIONS:

- a. Purchases of cloud services must comply with the City’s Purchasing Policy (Administrative Order No. 2013-06, as amended and adopted contract and procurement policies), including the requirement for approval of the IT Director prior to entering into the contract.
- b. All agreements for cloud services must be reviewed and approved by the City Attorney’s Office prior to entering into the contract.

- c. All Cloud providers must fill out the Cloud Services Questionnaire prior to entering into a contract with the City.

Section 2. Deciding Whether to Use the Cloud

2.1 To determine the suitability of a cloud service, consider the context in which the City operates and the consequences of a data breach.

- a. Determine the **City's security objectives**. What are the security/privacy requirements for the particular department or use?
 - i. Consider whether the City would be harmed if data became publicly available, was lost or damaged, or became unavailable. Some mission-critical or highly sensitive data may only be suited for a private cloud, as described below.
 - ii. Is there any personally identifiable information (PII) involved? In addition to the security concerns, does providing data containing PII to the service provider comply with established industry standards for securing PII.
 - iii. Is data exchanged with the vendor encrypted while in transit and at rest?
- b. Consider the **deployment model** offered by the provider, which affects the City's level of control of its data.
 - i. **Public**: app made available to general public via the internet.
 - ii. **Private**: computing environment operated exclusively for the City, so City's data not mingled with other data center tenants.
 - iii. **Hybrid**: Data or services are located on city premises and in the cloud.
- c. Assess the cloud service's ability to meet the City's **E-discovery, records retention, and public records request** requirements.
 - i. How well does the service manage data? Does the service include tools to help us search for and move documents through the E-discovery or records-request process?
 - ii. Does the service ensure the ability to have timely and actual destruction of records in accordance with our records retention schedules?
- d. What **demands will the service place on City systems**?
 - i. How will City employees access the application?
 1. Web
 2. Mobile
 3. desktop

Section 3. Selecting a Vendor

- a. **Financial due diligence:**

- i. How is the financial health of the vendor? A bankruptcy could cause a serious loss of data or at least a disruption while the City transitions to a replacement vendor.
 - ii. Understand whether the vendor uses subcontractors or third parties in providing the service. If so, it is possible there could be “cascading” service level agreements that depend on each other, and will make evaluating the vendor’s service much more complicated.
- b. **Security due diligence:** Understand the technical security controls used by the provider.
- i. Require the vendor to provide documentation of controls and compliance based on third party certifications.
 - ii. Understand the provider’s process for:
 - 1. **Data recovery.** Must the City independently back up data before transferring to vendor? What backup does the vendor provide in case of serious service outage?
 - 2. **Handling security breaches.**
 - iii. **Where are data centers located?** Does the provider have a redundant, geographically separate data center? Are they located in the United States?
- c. **Service Level Agreement:** Having a service in the cloud is only good if it can be accessed:
- i. Make sure the agreement guarantees a high percentage of uptime and penalizes the provider if uptimes are not met.
 - ii. Make sure the agreement clearly defines that the City owns their data at all times and that the vendor is not entitled to use the data for their own purposes other than providing the promised services.
 - iii. Make sure the agreement includes provisions for getting City data back in a usable format in the event the vendor goes out of business or we end our relationship with the vendor.

Appendix C-Web Governance

Web Governance Policy

This policy supports the City’s vision and goals for our external web presence. It identifies where the City intends to go with web-related programs and how it intends to deliver high quality, understandable and useful web services.

Section 1. Vision for the City Website

The City will use the web to serve citizens, to open government to its citizens, increase transparency and to support the processes necessary to achieve the City’s Strategic Plan. The City’s website will offer information and secure processes for citizens transacting business with the City’s departments. When citizens interact with the City, they will be able to:

- Get the information or service they want in an easy and intuitive manner. Easily find understandable answers to their questions;
- Complete basic transactions online, such as filling out forms or applying for programs; and

- Get clear and accurate instructions on where to start a process and what happens next.

This is the vision that guides the City’s long-term goals and objectives for the website

Section 2. City Website Goals and Objectives

Goal 1. Improve the quality and ease-of-use of City websites by identifying and enhancing the efficiency of the most used tasks, making those tasks easier to find, and eliminating content that is outdated, redundant, and inaccurate. Users will be able to find information and processes without having to figure out which part of our City provides it.

To achieve this goal, the City will:

- Identify the most used (top) tasks;
- Improve the efficiency of the top tasks;
- Improve the design of the home page to make it easier to find the top tasks;
- Require department directors & managers to regularly review and certify that their web content is relevant, and is both current and accurate;
- Establish an annual review process to verify and enhance top tasks, making changes to the home page as top tasks change over time;
- Work across departments to consolidate and/or link top tasks to help citizens get complete information and follow logical sequences; and
- Use new/social media tools to inform and educate customers about our services.
- Increase Transparency and availability of documents whenever feasible.

Goal 2: Improve customer service by simplifying the City’s communication with citizens on City websites and through new media. Improvements will include changes to content organization, written content, and methods (e.g. social media, use of forms) of delivery.

To achieve this goal, the City will:

- Train all employees who routinely contribute to the website to write for the web, using the principles of plain language;
- Increase the number of processes or communications that can be initiated with web-based forms;
- Develop and implement a process to review and—where needed—rewrite web content to make it easier to understand and use; and
- Organize content that is not frequently accessed into documents that can be referenced as needed.

Goal 3: Maintain and improve the efficiency and effectiveness of the website through increased communication with the City employees involved in web content management. The objective of the

communication is to teach and ensure that the initially adopted website re-design elements will be upheld, over time; simple design, plain-language, top tasks, and process-based content.

To achieve this goal, the City will:

- Provide regular training, both on-demand and scheduled sessions, for all new web content editors. This training will address the technical aspects of using the Content Management System (CMS) and the branding, content, and other policies.
- Establish a quarterly meeting of all department content editors to review website status, progress on objectives, and to prepare plans. Plans will include discussion of tasks or “business” that is currently not conducted online and if/when/how, those processes should be automated.
- Create a semi-annual e-newsletter for all department content directors, acknowledging excellence in department web content & achievements and keeping them informed on the latest analytical data.

Section 3. Web Governance Structure

The City’s web presence is governed by the City Manager, and is delegated to the Information Technology (IT) Director. The IT Director is charged with responsibility for establishing and managing the processes needed to ensure a continuing effective external web presence. This is accomplished by working with departments that utilize the web as a major tool for conducting business with external stakeholders. Departments are responsible for the creation of their own content, in accordance with adopted rules and standards.

Department Content Management Teams:

- 1. Web Content Manager:** Each department must have at least one assigned Web Content Manager, responsible for the web presence for their respective departments and service areas. The Web Content Manager:
 - Oversees the content of that department’s webpages, to ensure currency, relevancy and accuracy.
 - Appoints the department’s approver(s) and editor(s) and credits their accomplishments via annual performance review.
 - Is accountable for the quality, relevance, and currency of department publications and documents.
- 2. Department Approver:** Each department shall have at least one person assigned as the approver for website content. The Department Approver:
 - Reviews and approves content that is ready for publication outside of the department.
 - Department’s quality advocate; communicates web governance policy, procedures, and guidelines to editors.

- The person who manages the content review for the department and works with editors to update the content.
3. **Web Editor:** Departments may have multiple employees assigned to edit content on their webpages. Only editors who have received formal training will receive access to the website CMS. A Web Editor:
- Develops web content for publication to webpages
 - Responsible for finding and fixing broken links on pages, changing content as situations warrant.

Section 4. Standards for City of Bozeman Web Pages

2. The City will maintain a unified website consisting of a single URL and domain name, a small number of standard web templates that must be used, and a consolidated server environment.
 - The City uses the domain of Bozeman.net for external-facing purposes. All City departments, divisions, programs, services, or other operating units of the City must use the official City domain: Bozeman.net. All sub sites that serve City programs must be entered through Bozeman.net with no other visible URL unless approved by the IT Director.
 - No department or group may purchase or acquire a different URL for the use or web-presence of any City department, advisory group or function without the approval of the IT Director.
3. The City website is the primary location for all City information. All information must be placed on the website prior to posting to social media. Web Editors must use the simultaneous post function of the new CMS to post to the website and appropriate social media channels at the same time. No content is to be posted to social media only.
4. Editors must use the City's Web templates (which include header and footer navigation bars) on all webpages.
5. Editors must use components when there is a component that is made for the type of content that is being produced i.e.
 - Documents must be loaded into the documents library component and then linked from the library.
 - Photos must be placed into the photo library component and then linked from the library.
 - FAQ types of content must be placed in the FAQ component.
 - Staff and facility directory information must be placed into the staff and facilities directory components ETC.
 - A list of components that are available and what their functions are will be provided to each web editor as part of the City Website Style Guide.
6. All Bozeman^{MT} logos will link back to the official home page or department page, as indicated. Use and presentation of logos will follow the City Brand Guidelines which will be included as part of the City Website Style Guide.

7. All webpages will be accessible to all citizens, especially including the visually challenged accessing the internet through non-traditional means.
8. All content must meet the standards established in the City Website Style Guide;
9. Standards for Links: Links to commercial and non-profit sites are permitted on an educational basis; however, the links themselves must not be misconstrued as advertisements (logos and trademarks are prohibited, even if permission is granted for their use by the organization, and even if the images are not links). The links must not be done in such a way as to give the appearance of the approval, support, or endorsement of the City. A disclaimer disavowing endorsement may be appropriate.
10. If a document you are linking to exists in the Laserfiche repository, the link should go directly to the Laserfiche location of the document. Do not upload a separate pdf of the document to the Vision CMS document center.
11. Professional-quality photography and video help make the City's website attractive and contribute to a positive image of the City. Use documentary-style images that capture authentic and vibrant interactions among residents and services. Avoid artificial looking or obviously posed photos whenever possible. Ensure that all photos used are actually of Bozeman and surrounding areas of the City. All photos used on the website must use "alt text" tags to maintain ADA compliance for those who are visually impaired.
12. To ensure against copyright infringement:
 - Use only City-owned photos, videos, and other images on the City's website.
 - Assume that visual content you find online is protected by copyright, and do not post it to the City's website.
 - The City may have a license to use visual content the City does not own – for example, certain visual content created by a consultant or other third party. Be sure to abide by any and all copyright license requirements, including attribution.
 - If you are uncertain about whether the City owns certain visual content or has a license to use it, please contact the IT Director and the City Attorney's Office.
13. All Web Editors are responsible for ensuring that links are live and tested. Links should take users to sites that have current and accurate information.
14. All Web Editors should be familiar with and follow ADA Accessibility Compliance guidelines. The City Web Developer will run all site pages through a W3C compliant validation product at least annually to ensure Section 508C and WCAG 2.0 AA compliance for the disabled.
15. Wherever possible, fillable forms should be made available online and placed into the forms component of the CMS. All new forms created in the CMS must be created as a fillable form. Fillable PDF's may be appropriate for some situations that require the citizen to provide physical printed copies. Online fillable forms will greatly improve our level of customer service and satisfaction while reducing workloads on staff.
16. Web analytics will determine the priorities of what data is placed on the website. Departments can request analytics specific to their departments from the Web Developer.
17. Any content or design for the website that is performed by non-city employees (i.e. contractors) must fully comply with all aspects of this governance document and style guide.

Recognition and Acceptance of both the City IT Use Policy.

I hereby acknowledge I have read and understand the City’s IT Use Policy, as well as the policies contained in the appendices incorporated herein including Social Media Use Policy, Policy for Cloud Service Agreements, and the Web Governance Policy. I agree to abide by these policies. I understand that if I violate these policies, I may face legal and/or disciplinary action.

I ALSO UNDERSTAND THAT ANY PERSONAL USE OF THE CITY’S NETWORK, EMAIL, INTERNET, COMPUTERS, AND CELL PHONES BY ME IS DONE WITH THE FULL EXPECTATION AND REALIZATION THAT MY PRIVACY INTERESTS ARE GREATLY REDUCED. I RECOGNIZE THAT IF I WANT TO MAINTAIN CONFIDENTIALITY IN MY PERSONAL USE I WILL NOT USE ANY CITY NETWORK, EMAIL, INTERNET, COMPUTER OR CELL PHONE FOR MY PERSONAL COMMUNICATIONS.

Name _____
Signature _____
Date _____

Employee Verification of Compliance with Sections 3.4, 6.6, and 6.7 Upon Return of Computer or Cell Phone to IT Department.

I hereby acknowledge that I have reviewed the computer and/or cell phone being returned herewith to the IT Department and have taken reasonable steps to ensure that information has been saved to the appropriate network location, authorized software application, or authorized cloud location in accordance with Sections 3.4, 6.6, and 6.7.

I understand that these steps are for the purpose of verifying that I have complied with Sections 3.4, 6.6, and 6.7 of the Information Technology Use Policy, which is necessary to for the City to meet its legal preservation obligations, but also to ensure that substantive information important to my position is being saved on the network for future use.

Name _____

Signature _____

Device Identification: _____

Date: _____