

City of Wyoming, Michigan
Administrative Policy

Department Information Technology	
Department Head Approval: <i>Caril Sheppard</i>	Date: July 18, 2013
City Manager Approval: <i>[Signature]</i>	Date: 7.22.13
Subject: Computer Operating and Security Policy	

This page intentionally left blank.

City of Wyoming
Information Technology Department
Computer Operating and Security Policy

I. INTRODUCTION.....	4
II. SECURITY/APPROPRIATE USE	4
Computer Users.....	4
Unauthorized Access.....	5
Computer Sabotage	5
Passwords.....	5
Password Selection and Protection	5
Snooping	6
Hackers / Social Engineering	6
III. CONFIDENTIALITY	7
General	7
Handling Confidential Information	7
Encryption.....	7
IV. PHYSICAL SECURITY	7
Locks / Computer Theft.....	7
Portable Devices.....	7
Virtual Private Network (VPN).....	8
Wireless Technology.....	8
V. Mobile Device Management.....	9
Purpose	9
Definition / Mobile Device	9
Responsibilities and Enforcement	10
City Owned Mobile Devices.....	10

City of Wyoming
Information Technology Department
Computer Operating and Security Policy

Personal Owned Mobile Devices.....	10
VI. PRIVACY	11
Monitoring Computer Communications and Systems	11
Blocking of Inappropriate Content.....	11
Lawsuits and Subpoenas.....	11
VII. EXTERNAL COMMUNICATIONS	12
Third Parties.....	12
Dangers of the Internet.....	12
Internet Connections.....	12
Downloading/Uploading Files.....	12
VIII. E-MAIL	12
Electronic Communications.....	12
Dangers and Pitfalls of E-mail.....	13
Forwarding Information.....	13
Spam.....	14
IX. SOCIAL NETWORKING	14
Purpose.....	14
Guidelines and Rules.....	14
Content of Posts and Comments.....	15
Security Threats.....	16
Records Management and Preservation.....	16
Conclusion.....	16
X. INTRANET (THE CITY'S INTERNAL WEB PAGE)	17

City of Wyoming
Information Technology Department
Computer Operating and Security Policy

XI. ADMINISTRATIVE MATTERS.....	17
Back-up.....	17
Copyright Infringement.....	17
Harassment, Threats, Discrimination and Inappropriate Material.....	17
Accidents, Mistakes and Preventive Measures.....	18
Unauthorized Changes to City of Wyoming Computers.....	18
Acquisition of Computer Software and Equipment.....	18
Disposal of City Data.....	19
Disposal of City Computer Equipment.....	19
Personal Use of Computers.....	19
Proprietary Information.....	19
Reporting Policy Violations.....	19
Termination of Employment.....	20
XII. RECEIPT OF COMPUTER OPERATING AND SECURITY POLICY.....	21

Terms:

- City of Wyoming or Employer (hereinafter referred to as 'City' or 'the City').
- Computer User or User (defined as Employee, Volunteers, Representatives, Members of Council, Board and Commission Members or others having access to use a city computer).
- Information Technology (hereinafter referred to as 'IT').

Conditions:

- Information Technology staff, in the course of their job performance, are exempt from specific rules.
- Use of network sniffers shall be restricted to IT system administrators who must use such tools to solve network problems. Auditors, in the performance of their duties may also use them. They must not be used to monitor or track any individual network activity except under special authorization as defined by City policy that protects the privacy of information in electronic form.

Policy Created / Updated:

July 18, 2013
August 02, 2011
February 15, 2008
January 13, 2005

**City of Wyoming
Information Technology Department
Computer Operating and Security Policy**

I. Introduction

The purpose of the Computer Operating and Security Policy is to help protect the City of Wyoming and City of Wyoming computer users from liability and business interruptions due to inappropriate use of City computers and breaches of computer security.

This policy documents the computer users' responsibility to safeguard computer equipment and information from accidental or deliberate unauthorized access, tampering, snooping, distribution, or destruction. It sets forth what is, and is not, appropriate use of City computers. Users may be disciplined for noncompliance with City policy. This policy does not purport to address every computer operating and security issue. In the event you identify an issue or situation that you are not certain how to deal with, ask your immediate supervisor or higher management dependent upon the need.

The first, best, and most important line of defense starts with our people!

It is unquestioned that a well-trained work force properly versed in computer operating procedures, and computer user security matters, will have the best chance of minimizing business interruptions due to inappropriate, negligent, or unethical use of City computers. For this reason, this policy replaces any other computer use policy that may have been issued by individual departments.

The City of Wyoming may add to, or change, the Computer Operating and Security Policy at any time. When the policy is changed, notices will be given to computer users and, if required under the City's collective bargaining agreement, to Union Representatives. Notice of policy changes must be approved by the Director of Information Technology and the City Manager. Notices will be in writing, distributed to computer users and/or sent via the City's email system. Please read the policy carefully and sign the **Receipt of Computer Operating and Security Policy form** attached. The signed form must be submitted to the Human Resources Department for placement in your personnel file.

Keeping technology current is essential in order to provide opportunities for the City and its employees to impart a high level of customer service. In that same vein, it places the City at considerable risk. Implementing new technologies is expensive, time consuming, and without established policies and practices in place, could lead to disaster.

II. Security/Appropriate Use

Computer Users

Computer users are responsible for the appropriate use of City computers and/or portable devices and for taking reasonable precautions to secure the information and equipment entrusted to them. Users shall report inappropriate use of City computers and/or portable devices and breaches of computer security to an immediate supervisor or higher management dependent upon the situation. Users are responsible for adhering to City policies and practices as described herein, and to ensure City computers and/or portable devices are used in accordance with City policy guidelines, and reasonable measures are taken to prevent loss or damage of computer information and equipment.

**City of Wyoming
Information Technology Department
Computer Operating and Security Policy**

Unauthorized Access

Unauthorized access or attempt to access City computers is prohibited. Using a City computer to attempt unauthorized access of non-city computers is also prohibited. An individual not employed by the City of Wyoming, such as a contracted vendor or volunteer, who requests access to the network, must contact Information Technology management to establish a guest account.

Any form of tampering, including snooping and hacking, to gain access to computers is a violation of City policy and carries serious consequences. Users are required to turn their computer off or log out at the end of the day, and should either log-off or lock the keyboard when not in use for an extended period of time. This will help prevent computer security breaches and damage due to power surges.

Computer Sabotage

Destruction, theft, alteration, or any other form of sabotage of City computers, programs, files, or data is prohibited and may subject the violator to criminal prosecution.

Passwords

Simple password guessing is still the most prevalent and effective method of system penetration. In the event that someone guesses your password and logs in as you, not only are you at risk, but the City is placed at risk. It is the City's policy to change passwords minimally every (90) days. Computers often contain confidential information. If this information is accessed and distributed, it could cause great harm to you or someone you work with. Once someone gets your password, they have the capacity to, among other things:

- ◆ Send e-mail to individuals, or groups, representing themselves as you.
- ◆ Disseminate your files over the Internet.
- ◆ Delete or alter files.
- ◆ Share your password with other interested parties.
- ◆ Monitor your work.

Password Selection and Protection

Select difficult passwords and protect them from snoopers. A lot of damage can be done if someone gets your password. Users are responsible for password selection and protection. If you have a question about password selection or safekeeping, please contact the IT department via the Help Desk.

Do not: share your password with anyone, log on to your system if someone can see you keying in your password (there is no need to create the temptation), write it down where someone can find it, send it over the Internet, Intranet, e-mail, dial-up modem, or any other communication line.

It is not uncommon for employees to try to figure out a friend or an associate's password, just to see if they can. However, the same employee would never steal the key and go through your desk drawer, looking at everything private and confidential. Yet, this is what happens when passwords are cracked. This activity is strictly prohibited.

Good passwords are still the most effective computer security available to defend against unauthorized access. However, good passwords are only effective when used properly.

City of Wyoming
Information Technology Department
Computer Operating and Security Policy

Many of the City's computer systems are configured for strong passwords and will only accept passwords that are of a certain length and mixed character case. For example, the computer network login must be at least eight characters long, and contain at least three of the following four categories: one lower-case letter, one upper-case letter, one digit, and one special character. An example of a strong password is WyOmlngMi, as it meets all of the aforementioned requirements.

Snooping

Snooping (defined in Webster's Dictionary as 'to pry about in a sneaking way') into City computer systems is a serious violation of City policy. If you have no business being there, don't go there. If you accidentally identify a new way to access information, report it to management. Looking at computer data that does not belong to you is prohibited. Obtaining, or trying to obtain, other users' passwords, or using programs that compromise security in any way for the purpose of snooping, are violations of City policy. If you observe someone snooping, report it to an immediate supervisor or higher management dependent upon the situation. The City reserves the right to monitor and review any activity on City computers.

Hackers / Social Engineering

Social engineering is the art of manipulating people into performing actions or divulging confidential information. This is a type of confidence trick for the purpose of information gathering, fraud, or gaining computer system access. Never give confidential information about computer systems out over the telephone, or in any other way. If someone requests such information, get their name and phone number, and report the incident immediately to IT management. Legitimate release of this information must be authorized by an IT supervisor.

Using hacker programs and trying to access computer systems using hacker techniques is prohibited. Trying to hack into third party computer systems using City computers is prohibited. Hacker crimes result in millions of dollars of downtime, lost data, and other problems. Hacking is a serious offense. If you identify any vulnerability in the City's computer security system, report it to the IT Department.

Viruses (computer program that is part of another program and inserts copies of itself).

Worms (computer program that invades computers on a network, replicates itself to prevent deletion and interferes with the host computer's operation).

Trojan horses (computer program containing a hidden function that causes damage to other programs).

It is critical that users make certain that data and software installed on City computers are free of viruses. Information Technology staff or other individuals trained by IT staff (before installation) must scan data and software that have been exposed to any computer other than City computers. This includes downloads from the Internet and other sources of data that may be contaminated. Viruses can result in significant damage, and lost productivity. A computer can be infected when it accesses a malicious web page. Therefore, the easiest way to avoid such an issue is to only use trusted websites. If you are uncertain whether data or software needs to be scanned before installation, see anyone from the IT department.

The use of virus, worm, or Trojan horse programs is prohibited. If you identify a virus, worm, or Trojan horse, or what you suspect to be one, do not try to fix the problem. Immediately turn your computer off by pressing the power button, make notes as to what you observed, and contact the Information Technology Department. The principal concern is stopping the contamination before additional damage is done. These programs are most successful when ignored. They are designed to easily hop from application to application, contaminate a computer disk, and access another computer. They easily travel down phone, cable, ISDN, or other

City of Wyoming
Information Technology Department
Computer Operating and Security Policy

communication lines, infect e-mail, data and files, and find their way to other computer systems. The key to containment is limiting the reach of the contamination. Turning off your computer does this best.

III. Confidentiality

General

All computer information is considered confidential unless you have received permission to use it. Accessing or attempting to access confidential data is strictly prohibited. Confidential information shall only be used for its intended purpose. Using confidential information for anything other than its intended use is prohibited, without prior management approval.

Handling Confidential Information

Confidential information stored on computers requires coordination with IT to insure proper security and confidentiality. As such, it is important that users take extra care with confidential information stored on computers. The following actions may breach confidentiality:

- ◆ Printing to a printer in an unsecured area where documents may be read by others.
- ◆ Leaving your computer unattended with confidential files open.
- ◆ Leaving computer data/media/USB sticks with confidential data unattended, in easy to access places.
- ◆ Sending confidential information over the Internet, Intranet, dial-up modem lines, or other unsecured communication lines without approval from departmental management and/or IT management.

Encryption

Definition: To convert computer data and messages to something incomprehensible by means of a key so that can be reconverted only by an authorized recipient holding the matching key.

Encryption, encryption utilities and file compression utilities are prohibited without IT management approval. If you need to send confidential or proprietary information over the Internet or other public communication lines, you must obtain prior approval.

IV. Physical Security

Locks / Computer Theft

Physical security is key to protecting your computer and computer information from loss and damage. Media and other sensitive information should be stored in a locked drawer. Turn off your computer, log out or lock the keyboard when not in use for an extended period of time.

Portable Devices

- ◆ Portable devices that are asset tagged and 'borrowed' from the City must be signed out with the Information Technology Department or the issuing department if not through Information Technology.
- ◆ Report lost or stolen portable devices immediately to management.
- ◆ When traveling, devices must be in sight at all times or physically secured.

**City of Wyoming
Information Technology Department
Computer Operating and Security Policy**

- ◆ Safeguard portable devices and information from theft or damage. It is strongly recommended to password protect your cell phone, so if lost, it will not be wide-open (allowing access to stored documents, etc.) to whoever finds it.
- ◆ Prohibit access to devices (including family, friends, associates, and others) for any purpose, without management authorization.
- ◆ Adhere to all computer policies and practices of the City of Wyoming for on-site users.

Virtual Private Network (VPN)

It is the policy of the IT department to safeguard the security of all Information Technology assets belonging to the City of Wyoming, including those assets accessible using a Virtual Private Network.

A VPN utilizes public telecommunications networks to conduct private data communications. Most VPN implementations use the Internet as the public infrastructure and a variety of specialized protocols to support private communications through the Internet.

Requirements for VPN access:

- ◆ VPN access shall be limited to City of Wyoming owned computers. Access to non-City computers will be evaluated on a case-by-case basis by the IT Director.
- ◆ VPN access will be limited to computers with high-speed broadband capability due to the high overhead associated with VPN security protocols. Dial-up access is not generally appropriate for VPN access.
- ◆ The Department Director shall notify the IT department when a VPN is no longer required on a computer.
- ◆ Each computer will be granted VPN access for the minimum time necessary to accomplish the job, but for a period of time not to exceed one year.
- ◆ Each computer with VPN access shall be physically safeguarded to ensure no unauthorized person can access the City's resources.

The Department Director must submit a written request (VPN Access Request Form located on the City Intranet under Forms) for VPN access to the Information Technology Director. This request shall include:

- ◆ Identification of the specific data and/or system for which access is required.
- ◆ Identification of the computer requiring VPN access.
- ◆ Name of the person that will be using the VPN access.
- ◆ Expected duration of the VPN need (not to exceed one year & must submit a new request if the VPN access continues beyond the expected duration specified in the initial request).

The IT Director or designee will review each Department Director request and will:

- ◆ Upon approval, arrange for verification that the computer is compatible with the software necessary to establish secure VPN access and that the computer meets required security standards.
- ◆ Verify that the person using the VPN is provided the necessary user identification, password and training.
- ◆ Upon disapproval, return the request to the Department Director with a written explanation.

Wireless Technology

Today's information networks are exposed to an increasing demand for mobile information. The advent of wireless technologies introduces many benefits to users of information networks, some of which are:

**City of Wyoming
Information Technology Department
Computer Operating and Security Policy**

- ◆ Increased efficiency of users' access to information while not at their principal places of operations.
- ◆ Ease of use in sharing information.
- ◆ Increased productivity due to the accessibility of information, regardless of the individual's location.

Unauthorized monitoring of wireless transmissions is very easy. In addition, it is almost impossible to determine when, or if, someone is intercepting wireless traffic. Accordingly, wireless users are urged to exercise extreme caution with respect to confidential, proprietary, and personal information.

City of Wyoming wireless access requirements:

- ◆ Only approved wireless interface devices will be permitted to access the City's wireless network.
- ◆ Wireless adapter software will be configured by the City's IT staff with appropriate security settings.
- ◆ Using wireless is certainly an option, but realize that the reliability is not as good as utilizing a wired network connection at 1000 Megabyte/Second to a dedicated workstation. The wired connection provides much greater speed than the wireless (11-54 Megabyte/Second - shared bandwidth) connection.
- ◆ Wireless vendor access will consist of using separate wireless access point security, must be approved by IT, and the security for vendor access will be changed frequently.
- ◆ All computers connected to City's network via wireless must comply with the City's Computer Operating and Security policy.
- ◆ Only City of Wyoming IT staff (and approved/authorized Vendors) has the authority to install wireless access points. Any unauthorized access points will be immediately disconnected and IT staff will take possession of the unit. All information regarding the unauthorized access point will be routed to the proper management authorities to investigate.

V. Mobile Device Management

Purpose

The purpose of this section is to establish guidelines as to the appropriate use, security, support of, and employee responsibilities for the use of mobile devices whether owned solely by the City of Wyoming or owned by the employee. These guidelines also include the use of intellectual property used, downloaded, stored, etc. by mobile technology and communication devices. Information used or stored on any mobile device shall be considered as important for security as any paper document in the operation of City business.

Up until recently, the traditional IT paradigm was fairly simple. IT provided employees with the necessary information tools so that productivity, manageability and security could always be maintained. Typically, this consisted of providing employees with a computer (desktop/laptop), and related applications that met specific IT standards. However, with the mass adoption of mobile technology and the widespread use of social media, a new trend in IT has emerged that brings new challenges of information security and control.

Definition / Mobile Device

Any device or medium not permanently connected to the City of Wyoming network used for the purpose of receiving, sending, or storing information. This may include, but is not limited to, cell phones, smart phones, tablets, iPads, laptops, USB thumb drives; and digital storage media (CD, DVD, Thumb Drives, hard drives, etc.).

City of Wyoming
Information Technology Department
Computer Operating and Security Policy

Responsibilities and Enforcement

If at any time any email enabled device is lost or stolen, the employee for whom the device is assigned is responsible for immediately reporting the loss to the Information Technology department. The IT department may then remotely disable, lock, and/or wipe the device, rendering the device inoperable.

All email enabled devices shall be required to automatically lock after a reasonable period of inactivity (no longer than 5 minutes) and must be password protected to unlock the device. This is to ensure that a device left unattended will not be able to access devices or information by parties not governed by this policy.

If at any point Information Technology discovers any downloaded application has, or has the potential to compromise security to the network, IT personnel shall disable, lock and/or wipe the compromised device as soon as possible, and render it unusable for network access.

City Owned Mobile Devices

City owned tablets and/or laptops will have access to email, calendaring, contacts, tasks and the City network.

All requests for the purchase of an iPad (or similar type device) must also include a written business plan. A business plan is a formal statement of a set of business goals, the reasons they are believed attainable, and the plan for reaching those goals. It may also contain background information about prior attempts to reach goals that were unsuccessful due to equipment and/or functionality. The business plan will be reviewed by the City Manager and/or designee(s) and the request will either be approved or denied.

Personal Owned Mobile Devices

A personal mobile device will ONLY have access to email, calendaring, contacts and tasks.

The Information Technology Director or designee shall oversee all written requests to enable the use of personal mobile devices to access City resources. The Department Director must submit the written request (Personal Owned Mobile Device Request form located on the City Intranet under Forms) to the IT Director. Once approved, IT staff will make a reasonable effort to connect the device to the City's system and will verify that the computer meets required security standards. If not approved, the request will be returned with a written explanation.

All information contained on any personal device shall be considered as public record and subject to (but not limited to) open records requests, court discovery, investigations, etc.

At no time may a personal device enabled with access to any City network resource (such as email) be used by any personnel other than the employee granted access. (Example: If the City enables your iPad with City email, you must not share your iPad with a spouse, child, friend, neighbor, colleague, etc.) Employees shall not share passwords with anyone.

The IT department will not provide technical support for any personal mobile device, except to provide initial setup, security, and/or may wipe devices when needed to ensure the security and integrity of the City network. Employees are encouraged, during off hours, to utilize the Internet and/or the device manufacturer resources for any problem resolution with their personal mobile device.

**City of Wyoming
Information Technology Department
Computer Operating and Security Policy**

VI. Privacy

Monitoring Computer Communications and Systems

Many people assume data stored on computers, transmission of data between individuals on dial-up modem lines, communications on the Internet, voice mail and e-mail are private, and in some cases they are. However, it is management's fiduciary responsibility to monitor computer activity in order to:

- ◆ Provide a professional work environment where computer misuse is not tolerated.
- ◆ Reduce the risk of liability and business interruption to the organization.
- ◆ Establish and enforce policy to help prevent the violation of illegal acts and individual rights.

The City reserves the right, without prior notice, to access, disclose, use, or remove both business and personal computer communications and information, and will do so for legitimate business purposes.

Random audits to verify that City computers are clear of viruses, and used in accordance with City policy, will be performed. The City will investigate complaints about inappropriate images on computers, inappropriate e-mail, or other inappropriate conduct. The City may monitor Internet activity to see what sites are frequented, duration of time spent, files downloaded, and information exchanged.

Again, computer systems, telephone systems and information are City property, and shall be used principally for business purposes. Employees shall not maintain any expectation of privacy while using City computer or telephone equipment.

Blocking of Inappropriate Content

The City of Wyoming may use software to identify use of inappropriate Internet sites. Access to such sites may be blocked from access by City networks. In the event you encounter inappropriate or sexually explicit material while browsing on the Internet, immediately disconnect from the site, regardless of whether the site was subject to City blocking software. Reoccurrence of inappropriate web sites shall be reported to the Information Technology department.

Lawsuits and Subpoenas

City computers, like any other City property, are subject to the Freedom of Information Act and court order subpoenas. This means that anyone through the appropriate legal channels may access City computers, and the information contained in them. It is not difficult to imagine how easy it would be to find embarrassing and possibly incriminating information on City computers.

Management's intention is to ensure that users conduct their work to the highest ethical standard with the knowledge that computer information (even deleted files) can be used against you and the City of Wyoming in a legal proceeding or publicly revealed through the media. Suffice it to say, avoid keeping personal information not related to work in your computer files and keep your communications and data storage in a professional manner.

City of Wyoming
Information Technology Department
Computer Operating and Security Policy

VII. External Communications

Third Parties

The same standards of decorum, respect, and professionalism that guide us in the office environment apply to computer communications with third parties. Important, confidential, and proprietary information is stored on City computer systems. Management must approve computer data and other information received by, or provided to, third parties. Please keep in mind that third parties may have a legitimate business need, duty, legal right, or obligation to access, disclose, or use information transmitted.

Dangers of the Internet

Web sites, data and images found on the Internet may be subject to copyright law. Therefore, use of such by City employees could be a potential liability. Viruses can be downloaded from the Internet. Inappropriate web sites, images, and communications exist on the Internet. As such, users must follow established computer operating policies and practices to reduce the opportunity for security breaches, and inappropriate or illegal activity resulting from connecting to the Internet.

The City of Wyoming is not responsible for material viewed or downloaded by users from the Internet. Users are cautioned that many of these pages may include offensive, sexually explicit, and inappropriate material. Users accessing the Internet do so at their own risk.

Internet Connections

Internet connections are authorized for specific business needs only. The following activities are prohibited without prior IT staff authorization and programs/access may be removed by IT staff when discovered in the course of their job performance:

- ◆ Downloading shareware, freeware and other copyrighted materials.
- ◆ Copying programs, files, and data to the Cloud.
- ◆ Transmitting important, confidential, or proprietary information.

Individuals that have received management approval to transmit information on the Internet should understand that such transmissions are identifiable and attributable to the City. The Internet should be considered a public forum for all transmissions. All communications on the Internet provide an opportunity for a permanent record, and can be edited and retransmitted. Accordingly, maintain a professional decorum in all communications and transmissions.

Downloading/Uploading Files

Downloading or uploading confidential or proprietary information requires approval by departmental management and Information Technology management.

VIII. E-mail

Electronic Communications

E-mail is a wonderful tool. Used correctly, it can provide significant efficiencies, and improve the quality of the way we do business. It makes dissemination of information easy and cost-effective. The City provides the

**City of Wyoming
Information Technology Department
Computer Operating and Security Policy**

majority of users with access to City email, therefore the use of personal email accounts or services are prohibited.

The same standards of decorum, respect, and professionalism that guide us in our face-to-face interactions apply to the use of e-mail. The City may append email headers or footers indicating our commitment to these standards.

Minimal and/or occasional use of e-mail for personal reasons is permitted. However, only City computer users are allowed access to the City e-mail system. The following e-mail activity is prohibited:

- ◆ Accessing, or trying to access, another user's e-mail account.
- ◆ Obtaining, or distributing, another user's e-mail account credentials.
- ◆ Using e-mail to harass, discriminate, or make defamatory comments.
- ◆ Using e-mail to make off-color jokes, send inappropriate e-mail, material or content.
- ◆ Transmitting City records within, or outside, the City without authorization.
- ◆ Transmitting junk mail, chain letters, or soliciting for commercial, religious, charitable, (unless sanctioned by the City e.g., United Way) or political causes.

Employees shall report inappropriate use of e-mail to an immediate supervisor or higher management person dependent upon the situation.

Dangers and Pitfalls of E-mail

Appropriate e-mail etiquette is essential to maintaining a productive and professional work environment. Comments that might be made at parties, in elevators, and on the telephone are now done via e-mail. However, e-mail does not disappear into thin air. It can be widely, easily, and quickly disseminated. E-mail can be edited, forwarded, distributed, and filed for later use, possibly at the most inopportune time. For professionals with electronic recovery skills, e-mail is a gold mine. If you would not put it in a memorandum on City letterhead, do not say it with e-mail.

Forwarding Information

E-mail makes attaching files and forwarding data a snap. However, the damage from forwarding something to the wrong person may be serious. Please take a minute to think through the appropriateness of all the parties you are forwarding. If you receive an e-mail (particularly e-mail with an attachment) and intend to forward it to others, consider the following:

- ◆ Is any of the information unnecessary or inappropriate for any individual?
- ◆ Would the author take exception to, or be embarrassed by, your forwarding the information? (a good rule of thumb is to copy the author).
- ◆ Might the information be received negatively?
- ◆ Might the information be misunderstood?
- ◆ Is the receiver likely to forward the information to individuals that should not have, or do not need, the information?
- ◆ Do the attachments have viruses?

If the answer to any of these questions is yes, do not forward the information. Edit it, or create a new file. A bad decision may result in misunderstanding, hurt feelings, and added work.

City of Wyoming
Information Technology Department
Computer Operating and Security Policy

Spam

Sending unsolicited messages or files to individuals, groups or organizations that you do not have a prior relationship with is prohibited, without written authorization from your supervisor. Sending messages or files with the intent to cause harm or damage to the intended receiver is a violation of City policy and in addition to violating work rules, may result in criminal prosecution.

IX. Social Networking

Purpose

The role of technology in the 21st century workplace is constantly expanding and now includes social media communication tools that facilitate interactive information sharing, interoperability, and collaboration. Moreover, a social networking presence has become a hallmark of vibrant and transparent communications. Social networking improves interactivity between a city agency and the public, and it reaches populations that do not consume traditional media as frequently as others do. Therefore, City departments may enhance their communications strategies by using social networking web sites.

When you are participating in social networking, you are representing both yourselves personally and the City of Wyoming. While we encourage this online collaboration, we would like to provide users with a set of guidelines for appropriate online conduct and to avoid the misuse of this communication medium.

Guidelines and Rules

The goal of authorized social networking and blogging is to become a part of the industry conversation and promote web-based sharing of ideas and exchange of information. Authorized social networking and blogging shall be used to convey information about City services and promote and raise awareness of the City, communicate with citizens, businesses and visitors, issue or respond to breaking news, and discuss City and department specific activities and events.

However, prior to the creation and management of any social networking activity relevant to City business, any/all users must first obtain written approval from the City Manager. Once authorization is received, the City Communications Specialist (or City Manager designee) will coordinate all requests for usage and maintain a list of all social networking application domain names in use as well as associated user identifications and passwords. Should the user who administers the account be removed as administrator or no longer be employed by the City, the Communications Specialist (or City Manager designee) should immediately change all passwords and account information to maintain City control.

The City Manager and designees are authorized to remove any content that does not meet the rules and guidelines of this policy or that may be illegal or offensive. Removal of such content will be done without permission or advance warning to the poster or the blogger.

Each City social networking site shall include an introductory statement which clearly indicates it is maintained by the City and shall have City contact information prominently displayed. Where possible, social networking sites should link back to the official City of Wyoming internet site for forms, documents and other information.

When you participate in social media, stay within your area of expertise and provide unique, individual perspectives on what is going on at the City, and in other larger contexts. Post meaningful, respectful comments, no spam, and no remarks that are off-topic or offensive. Do not use social networking sites for political purposes, to conduct private commercial transactions, or to engage in private business activities. Pause

City of Wyoming
Information Technology Department
Computer Operating and Security Policy

and think before posting. Reply to comments in a timely manner, when a response is appropriate. Respect proprietary information, content, and confidentiality. When disagreeing with others' opinions, keep it appropriate and polite.

Ensure that your participation is consistent with the provisions of the City's Rules and Regulations Regarding Employee Personal Conduct and know and follow the City's Computer Operating and Security Policy.

Content of Posts and Comments

Transparency: Your honesty will be quickly noticed in the social media environment. If you are blogging about your work at the City, use your real name, identify that you work for the City, and be clear about your role.

Judicious: Make sure your efforts to be transparent do not violate the City's privacy, confidentiality, and any applicable legal guidelines for external communication. Never comment on anything related to legal matters, litigation, or any parties the City may be in litigation with. Posting photographs of other employees, clients, vendors or suppliers requires prior authorization unless the person is participating in a public event setting.

Comments containing any of the following forms of content shall not be allowed: (1) comments in support of or opposition to political campaigns or ballot measures; (2) any personal attacks; (3) content that promotes, fosters, or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, status with regard to public assistance, national origin, physical or mental disability or sexual orientation; (4) sexual content or links to sexual content; (5) conduct or encouragement of illegal activity; (6) information that may compromise the safety or security of the public or public systems; or (7) content that violates a legal ownership interest of any other party.

Any content removed based on the above guidelines that meets the definition of a public record must be retained, including the time, date and identity of the poster when available in accordance with the retention schedule and rules set by the State of Michigan.

Be smart about protecting yourself, your privacy, and any sensitive or restricted confidential and sensitive information. What is published is widely accessible, not easily retractable, and will be around for a long time, so consider the content carefully.

Conversational: Talk to your readers like you would talk to people in professional situations. Avoid overly composed language. Bring in your own personality and say what is on your mind. Consider content that is open-ended and invites response. Encourage comments when appropriate. Share with the participants the things we are learning and doing, and open up social media channels to learn from others. You may encounter comments which cause you concern as a moderator or responsible party. If user content is positive or negative and in context to the conversation, then the content should be allowed to remain, regardless of whether it is favorable or unfavorable to the City. The City cannot guarantee the accuracy, completeness, or usefulness of any third-party post. The City does actively monitor posts, but is not responsible for the content of posts. A third-party post expresses the views of its author and does not represent the views of the City.

Value: The best way to get your content read is to write things that people will value. Social communication from the City should help residents, partners, and co-workers. It should be thought-provoking and build a sense of community. If it helps people improve knowledge or skills, build their businesses, do their jobs, solve problems, or understand the City better, then it is adding value.

City of Wyoming
Information Technology Department
Computer Operating and Security Policy

Responsibility: What you write is ultimately your responsibility. Participation in social computing on behalf of the City is not a right, but an opportunity. Treat it seriously and with respect. Follow the terms and conditions for any third-party sites. Users can be held personally liable for commentary that is considered defamatory, obscene, proprietary or libelous by any offended party, not just the City of Wyoming.

Security Threats

It is important to note that security related to social media is fundamentally a behavioral issue, not a technology issue. In general, users unwittingly may provide information to third parties and pose a risk to the core City network. Prevalent social media security risks include third-party spear phishing (an attack targeting a specific user or group of users, attempting to deceive the user(s) into performing a routine action, such as opening a document or clicking a link, which the phisher has booby-trapped to launch an attack), social engineering (an attack that involves gathering and using personal information about a target in a deceitful manner in order to convince the target to provide the attacker permissions to obtain or access restricted information), spoofing (involves one person, system, or website successfully masquerading as another by falsifying identity-related information and thereby being treated as a trusted user or system by another user or program), and web applet attacks (code routines, scripts or utilities that interact dynamically with web pages to provide additional functionality to the user).

Because of the importance of proper operation of the City network and the sensitivity of information stored on City systems within the network, a City user must never use a current City password as a password on any other site. Also, users shall not post/discuss sensitive information such as data files that were not specifically created for public release, dump files, log data, network diagrams, configuration files, City seals, logos or trademarks, any copyrighted information where written reprinted information has not been obtained in advance, and user names and passwords.

In addition, employees must not link from a personal blog or social networking site to the City of Wyoming's internal or external web site.

Records Management and Preservation

Content placed by the City on social networking sites is subject to the Freedom of Information Act or legal discovery provisions while it is retained according to the City's Records Retention and Disposal Schedule. Web sites or social media sites are not designed or intended to preserve records as required by the Schedule. Records required to be maintained pursuant to a relevant records retention schedule shall be maintained for the required retention period in a format that preserves the integrity of the original record and is easily accessible using the approved City platforms and tools.

In the spirit of transparency in local government, account administrators and/or the City Communications Specialist who receive messages through the private message service offered by the social media site shall encourage users to contact them at a public e-mail address maintained by the City. For private messages that the account administrators and/or City Communications Specialist do receive, they shall be treated as constituent e-mails and therefore, as public records. Account administrators or other authorized staff members shall reply using their City e-mail account.

Conclusion

Remember, the overall goal of the social media policy is to protect the rights and privacy of all users and the integrity and reputation of the City.

**City of Wyoming
Information Technology Department
Computer Operating and Security Policy**

X. Intranet (The City's Internal Web Page)

The City Intranet, like e-mail, is a wonderful tool. It can provide significant efficiencies; and it makes dissemination of information easy and cost-effective.

Data, programs, and other information are updated regularly on the City Intranet. As such, it is your responsibility to ascertain that information you are working with is current.

The same standards of decorum, respect, and professionalism that guide us in the office environment apply to the use of the Intranet. Important, confidential, and proprietary information is stored on the Intranet. Accordingly, only City personnel are allowed access to the Intranet, without written authorization from management. All City policies apply to use of the Intranet. The following activities are prohibited, without management authorization:

- ◆ Installation of a web site, page, or any other information.
- ◆ Installation of business or personal software on the Intranet.
- ◆ Unauthorized access/sharing of Intranet programs, data, and files.
- ◆ Assisting anyone outside the City in obtaining access to the Intranet.
- ◆ Making any changes to the Intranet hardware or software.

XI. Administrative Matters

Back-up

It is recommended that all important, confidential, or proprietary information be stored on the local area network (LAN). Storing information on your desktop computer is not recommended and makes the user responsible for regular (daily) back up of essential computer files, and the secure storage of back-up media. The LAN is equipped with electronic and physical security. Activity on the network is monitored for tampering, and other security breaches. Maintenance and back up are performed on the LAN daily. Programs and other information are updated on the LAN regularly. Use the LAN; it is safe, effective, and reliable.

Copyright Infringement

The City of Wyoming does not own computer software, but rather licenses the right to use software. Accordingly, City licensed software may only be reproduced by authorized City officials in accordance with the terms of the software licensing agreements. Unauthorized copying, redistributing, and republishing of copyrighted or proprietary material is strictly prohibited. Copyright laws apply on the Internet as well. There is no 'but copying it was so easy' defense to copyright infringement. Copyright infringement is serious business, and the City strictly prohibits any such activity. If you have questions about copyright infringement, discuss it with IT management immediately.

Harassment, Threats, Discrimination and Inappropriate Material

It is City policy, and federal and state law that allows employees to work free of harassment, threats, and discrimination. Harassment is behavior directed towards an individual due to their race, age, marital status, gender, disability, religion, national origin or any other reason prohibited by law for the purpose of interfering with an individual's work performance, or creating an intimidating or hostile work environment.

City of Wyoming
Information Technology Department
Computer Operating and Security Policy

Users may receive files, data, pictures, games, jokes, etc. that may be considered offensive. The computer is possibly the easiest tool for obtaining, storing, sharing, and disseminating to large audiences such material and viewpoints. It is inappropriate to use City computers to share your personal views about religion, politics, sexuality, or any other subject of a personal nature that could be considered offensive to others within or outside the workplace. Computer users may not purposely access or attempt to access web sites that contain sexually offensive material. Be advised that such activities may violate the City's harassment policy and other work rules.

Computers provide a huge potential for unlawful harassment. Users often think their communications are private, and trashed or deleted files are gone forever. Information on City computers is not necessarily private and deleted files are often easily recovered. Users often feel comfortable writing and storing files within the confines of their 'personal' computer, and sharing personal views on a wide range of non-business subjects. Remember, whatever you transmit is a permanent record to the receiver. It can, at some future date, be taken out of context and used against you and the City of Wyoming.

Accidents, Mistakes and Preventive Measures

'An ounce of prevention is worth a pound of cure' is a very appropriate cliché for computer operations. Take a few seconds to read the computer screen before you delete, save, or transmit files. In addition, users need to take reasonable precautions with respect to computer operations, maintenance, handling, and transportation. Some of which include:

- ◆ Computer and telephone (ShoreTel-VoIP) equipment that has been established at a particular location must not be moved without prior authorization from the IT Department. This is essential for IT to maintain an accurate inventory of all City computer equipment for audit and replacement purposes.
- ◆ Surge protectors and/or extension cords for computer equipment must never be 'daisy chained or piggy backed' to one another, since this can cause an overload.
- ◆ Approval must be obtained from IT management prior to the utilization of any data jacks, since connection to an improper jack could result in damage (kill a switch, corrupt data) to the network.

Unauthorized Changes to City of Wyoming Computers

The City's computer systems have been designed and documented to prevent loss of data, and provide an audit trail for correcting problems. Unauthorized changes to computer systems may result in lost productivity. Installing software and making changes to computer hardware, software, system and configuration are prohibited, without prior IT management authorization. Any unauthorized and/or unlicensed software may be removed by IT staff during the course of their job performance.

Acquisition of Computer Software and Equipment

Acquisition of computer software and equipment are prohibited without prior approval from Information Technology management. All computer software and hardware purchases must be registered with the IT Department, meet pre-established quality requirements, and be compatible with other City computer software and equipment.

City of Wyoming
Information Technology Department
Computer Operating and Security Policy

Disposal of City Data

It is the User's responsibility to purge files that no longer have a practical use on a periodic basis. Old computer files, emails and the alike utilize disk space, and often represent a potential hazard to you and the City. Contact your Supervisor or the City Clerk for Records Retention storage requirements if uncertain when it is safe to delete files.

Disposal of City Computer Equipment

Sale and disposition of computer equipment (copy machines, telephones, cell phones, fax machines) shall be completed in accordance with the City Charter, Code, Purchasing Policy and the City's Theft Policy. Sale of property in excess of \$7,500 requires formal sealed bids and City Council approval. Sale and disposal of computer equipment must be authorized by the Information Technology Department.

Personal Use of Computers

Incidental and occasional personal use of City computers is permitted for reasonable activities that do not need substantial computer hard disk space, or other computer equipment. Computer users are expected to demonstrate a sense of responsibility and not abuse this privilege. As a general rule, if you would be uncomfortable asking for permission, it is probably not an appropriate use of City computers. Prohibited activities include, but are not limited to, entertainment software (including games), personal software and hardware, writing lengthy personal information (e.g. your autobiography) and running a personal business on the side. Using City computers to store or transmit inappropriate jokes, junk mail, chain letters, or to solicit for commercial, religious, charitable (unless sanctioned by the City (e.g. United Way)) or political causes is prohibited. If you are uncertain about a specific activity, ask your supervisor. Personal files, information, and use of City computers will be treated no differently by the City than any other business activity, with regard to employee privacy.

Proprietary Information

City data, databases, programs, and other proprietary information represent City assets and can only be used for authorized City business. Use of City assets for personal gain or benefit is prohibited.

Reporting Policy Violations

Computer users shall report violations, or suspected violations, of computer policy. Activities that are violations of this policy and must immediately be reported to an immediate supervisor or higher management person include, but are not limited to:

- ◆ Attempts to circumvent established computer security systems.
- ◆ Use, or suspected use, of virus, Trojan horse, or hacker programs.
- ◆ Obtaining, or trying to obtain, another user's password.
- ◆ Using the computer to make harassing or defamatory comments, or to in any way create a hostile work environment.
- ◆ Using the computer to view and/or communicate inappropriate materials, messages or jokes that may be considered offensive by others.
- ◆ Gambling or any other activity that is illegal, violates City policy, or is contrary to the City's interests.
- ◆ Trying to damage the City, or an employee of the City, in any way.
- ◆ Portraying yourself as someone other than who you are, or the City you represent.

**City of Wyoming
Information Technology Department
Computer Operating and Security Policy**

Computer policy violations will be investigated. Supervisors and Management are required to take appropriate action when violations of the computer policy may have occurred. Noncompliance with the City's computer policy may result in discipline up to, and including discharge. Users that report violations or suspected violations of City policy will be protected from termination, discrimination, harassment, and any other form of retaliation. Hackers, snoopers, password stealers, virus installers, data erasers, and anyone involved in such activity will be disciplined.

If you identify computer security vulnerability, you are required to report it immediately.

Termination of Employment

All information on City owned devices is considered City property. Deleting, altering, or sharing confidential, proprietary, or any other information upon termination of employment requires management authorization. Upon termination, any computer technology you have been entrusted with must be relinquished to your Supervisor with all passwords, identification codes, and any other appropriate information necessary to allow uninterrupted use.

The following activity is prohibited upon termination of employment and may subject the violator to criminal prosecution:

- ◆ Accessing City of Wyoming computers.
- ◆ Providing anyone else access to City computers.
- ◆ Taking computer files, data, programs, or computer equipment.

It is the responsibility of each department Director/Manager to immediately advise the Human Resources Department when a user terminates employment or affiliation with the City of Wyoming. The Information Technology Department will remove users from the City system(s) upon notification from Human Resources.

**City of Wyoming
Information Technology Department
Computer Operating and Security Policy**

XII. Receipt of Computer Operating and Security Policy

I have received and read the City's Computer Operating and Security Policy. I understand that I am responsible for adhering to the policies and practices described therein. I understand that the City may from time to time monitor and review any computer user or computer user's use of City computers, including but not limited to email, internet use, and any other files. I understand that these policies may be added to, or changed by the City at any time. It is my responsibility to bring any questions I have about the Computer Operating and Security Policy to my supervisor.

Date: _____

Computer User Signature: _____

Computer User Name (please print): _____

**CITY OF WYOMING INFORMATION TECHNOLOGY
PERSONAL OWNED MOBILE DEVICE REQUEST FORM**



User Name (Print):	User Windows Login:	Date of Request:
Department:	Division:	

Describe the device (Include Manufacturer, Model, Operating System, Memory, Anti-Virus, Firewall, Anti-Spyware Software):

Describe how you are intending to use the device:

<< Excerpt of Personal Owned Mobile Devices Policy from City of Wyoming Computer Operating and Security Policy >>

A personal mobile device will ONLY have access to EMAIL, CALENDARING, CONTACTS and TASKS.

The Information Technology Director or designee shall oversee all written requests to enable the use of personal mobile devices to access City resources. The Department Director must submit the written request (Personal Owned Mobile Device Request form located on the City Intranet under Forms) to the IT Director. Once approved, IT staff will make a reasonable effort to connect the device to the City's system and will verify that the computer meets required security standards. If not approved, the request will be returned with a written explanation.

All information contained on any personal device shall be considered as public record and subject to (but not limited to) open records requests, court discovery, investigations, etc.

At no time may a personal device enabled with access to any City network resource (such as email) be used by any personnel other than the employee granted access. (Example: If the City enables your iPad with City email, you must not share your iPad with a spouse, child, friend, neighbor, colleague, etc.) Employees shall not share passwords with anyone.

The IT department will not provide technical support for any personal mobile device, except to provide initial setup, security, and/or may wipe devices when needed to ensure the security and integrity of the City network. Employees are encouraged, during off hours, to utilize the Internet and/or the device manufacturer resources for any problem resolution with their personal mobile device.

ROUTING / APPROVALS	Approved
Requestor (signature):	
Department Head of Requestor (signature):	<input type="checkbox"/>
IT Director (signature):	<input type="checkbox"/>
Computer/Device Check Out and Approval: (Computer will be connected and checked for Up-To-Date and compatible operating system(s), antivirus, firewall and required security standards.)	<input type="checkbox"/>
IT Supervisor (signature):	
Request Denied: <input type="checkbox"/>	
Reason Denied:	